Lezioni di Storia della Matematica
(Versione preliminare, 2002 - 2003)

Massimo Galuzzi[1]

5 ottobre 2004

[1]e-mail: massimo.galuzzi@mat.unimi.it

Indice

Capitolo 1

Considerazioni introduttive

1.1 Cosa l'insegnamento della storia della matematica non è

Seguendo un modulo espositivo caro a Benedetto Croce,[1] si può cominciare con il dire che cosa l'insegnamento della storia della matematica non è (o non deve essere).

Questo insegnamento[2] non può ridursi all'uso di un manuale, per quanto ben fatto questo possa essere. Un manuale contiene (in genere) utili informazioni: gli *Elementi*[3] di Euclide sono composti di tredici libri. Di essi sei sono dedicati alla geometria piana. Il teorema di Pitagora è dimostrato nella proposizione I.47,...

Tuttavia, già quando affermiamo il 'dato di fatto' che Euclide non utilizza il quinto postulato[4] per le prime ventotto proposizioni del primo libro, è

[1] Si veda, ad esempio (Croce 1976). Molte delle considerazioni che seguono si trovano, sia pure in altra forma, nella mia *Premessa* a (Weil 2002). Ma si consiglia vivamente la lettura del testo stesso di André Weil.

[2] Le considerazioni che seguono si rivolgono all'insegnamento della storia in generale ma valgono,– mi sembra,– a maggior ragione, se vengono riferite ad una pratica di questo insegnamento intercalato, per così dire, nell'insegnamento, a varî livelli, della matematica stessa.

[3] Un'ottima traduzione italiana è (Euclide 1970), ristampata recentemente.

[4] È utile rammentare che la formulazione euclidea di questo postulato è: "Se una retta venendo a cadere su due rette forma gli angoli interni da una stessa parte minori di due angoli retti, le due rette, prolungate indefinitamente, si incontreranno dalla parte in cui i due angoli sono minori dei due angoli retti." La formulazione che si incontra in

doveroso accompagnare questo dato di fatto con una *interpretazione*. Ad esempio:

- Euclide già presagisce la possibilità di una geometria non euclidea e con le prime ventotto proposizioni si spinge innanzi in questa direzione.
- Per semplici motivi di eleganza formale, preferisce dimostrare alcune istanze più deboli di certe proposizioni (ad esempio la I.16, che afferma che un angolo esterno di un triangolo è maggiore di ciascuno degli angoli interni ad esso opposti.[5]
- Non possiamo argomentare in modo plausibile a partire da un testo che ha subito numerose modifiche nel corso di più di venti secoli. Può darsi che gli *Elementi* riflettano una 'sedimentazione' delle proposizioni che non riflette se non in modo impreciso la volontà euclidea.

Poiché la trasmissione reale del sapere non può che consistere nel comunicare ciò che è un nostro sicuro possesso, è chiaro che dobbiamo formare una nostra precisa opinione. Il che non può avvenire senza un confronto con il *testo* euclideo.[6]

Ancor più evidente e necessario diventa un confronto personale con il testo se si vuol suggerire un significato generale agli *Elementi*. Essi culminano con il tredicesimo libro, ossia con l'analisi dei poliedri regolari,– i solidi platonici,– e riflettono con ciò un evidente interesse per l'indagine platonica sulla natura delle idee matematiche o manifestano un evidente influsso aristotelico nella loro architettura logica?

Da secoli questo problema viene discusso, ed una qualsiasi ragionevole esposizione del contenuto degli *Elementi* non può prescindere da una precisa valutazione della loro natura.

---

molti libri moderni (spesso attribuita ad Euclide) è quella di Playfair (in realtà, come dice esplicitamente lo stesso Playfair nella sua edizione degli *Elementi*, la fomulazione è di Proclo): "Data una retta ed un punto esterno esiste una ed una sola parallela per il punto alla retta data". Si tratta di una formulazione nella quale si mescolano esistenza ed unicità.

[5]Questa proposizione è un ovvio corollario del teorema sulla somma degli angoli interni. Per la sua dimostrazione richiede la possibilità di raddoppiare un segmento arbitrario.

[6]Ed ancora, dietro la ovvietà di questa osservazione, si cela una scelta: potremo accontentarci di una traduzione in una lingua moderna del testo di Euclide o dovremo confrontarci con il testo greco? E quanto profonda deve essere la conoscenza di questa lingua? Un'utile lettura è comunque (Mugler 1958).

Ovviamente, non c'è ragione per la quale la nostra opinione su una questione matematica non venga a coincidere in fine, del tutto od in parte, con quella dell'autore di un buon manuale. Ma è cosa radicalmente diversa accettare passivamente l'opinione di Kline, o di Boyer o di Zeuthen, dall'esprimere un consenso fondato su una conoscenza dei testi che essi stessi hanno considerato.

Si può essere partecipi dell'opinione di Gino Loria, che vedeva in Descartes solo il precursore della moderna geometria analitica, ancora assai lontano dalla sua reale natura.[7] O si può sostenere un'interpretazione radicalmente contraria (che è quella di chi scrive[8]). Ma, in ogni caso, sarà assai poco significativo consentire con l'uno o l'altro giudizio senza un preciso riscontro con il testo cartesiano.

Quanto diversa efficacia possa avere la presentazione della geometria analitica accompagnata da informazioni storiche che siano un reale possesso del docente, piuttosto che la banale ripetizione dell'opinione di Loria, o dell'opinione contrapposta, è troppo evidente perché si debba soffermarsi su questo punto.

1.2 Storia e bellezza della matematica

È certamente desiderabile che molti amino la matematica, la sua razionalità, la sua bellezza. Ma così come non tutti amano la poesia o la musica,– od un certo genere di musica o di poesia,– allo stesso modo non è giusto pretendere che tutti partecipino dello stesso ardore intellettuale di fronte alla matematica.

Si consideri una delle prime 'scoperte' dei pitagorici. Si guardi la figura seguente

$$\begin{array}{cccc} * & * & * & * \\ * & * & * & * \\ * & * & * & . \\ * & * & . & . \end{array}$$

Essa esibisce in modo 'visivo' il fatto che la somma di numeri dispari succes-

[7]Si veda (Loria 1923).

[8]Si veda (Galuzzi 2002).

sivi fornisce i quadrati.[9]

$$1 + 3 = 4,\ 1 + 3 + 5 = 9,\ 1 + 3 + 5 + 7 = 16, \ldots$$

E l'immagine grafica è (forse) ben più convincente della identità

$$m^2 + 2m + 1 = (m + 1)^2.$$

Tuttavia, anche una comprensione piena e profonda di questa proprietà dei numeri interi, non necessariamente suscita il desiderio di scoprire altre proprietà della stessa natura. La fascinazione della teoria dei numeri, la regina della matematica, può non agire per tutti allo stesso modo. E chi non subisce questo fascino proverà una noia variamente graduata a sentir narrare di Pitagora e dei suoi adepti.

Se è giusto e necessario che tutti i cittadini raggiungano il (modesto) livello di conoscenze matematiche necessarie per la vita pratica, se è auspicabile che tutti giungano a possedere quegli strumenti di razionalità minimale che consentano poi di esprimere le proprie scelte politiche in modo consapevole, non ne segue come corollario che tutti debbano amare la matematica in pari misura.

Chi ama la musica, e per ciò desidera avvicinarsi alla pratica musicale, per esempio imparando a suonare uno strumento, sa che per raggiungere il fine desiderato, avrà bisogno di una certa tecnica: scale, scale per terza, scale cromatiche...

Eseguire una scala cromatica non è molto gratificante. Ma, sino ad ora, almeno, non è pratica diffusa far precedere, o far seguire, questo esercizio da informazioni sulla storia della musica che abbiano il fine di renderlo più attraente. E se è vero che nel periodo del predominio della tonalità, l'uso di cromatismi (soprattutto discendenti) serviva a comunicare un senso di smarrimento e di incertezza (come spesso accade nelle arie di Mozart) è ancor più vero che è la conoscenza tecnica che favorisce la comprensione storica e non viceversa.

Chi ha provato piacere nel giungere alla soluzione di un problema geometrico mediante l'uso di riga e compasso, proverà del pari piacere nell'apprendere che ogni problema geometrico, trattato algebricamente, è ancora risolubile con gli stessi strumenti se la sua soluzione dipende solamente dalla successiva soluzione di equazioni di secondo grado.

[9] Molte proprietà 'visive' dei numeri interi (e molto altro) si trova nell'affascinante volume (Conway and Guy 1999).

Ma il complesso di manipolazioni algebriche che consentono di ricondurre la soluzione di alcuni tipi di equazioni di grado superiore al secondo alla successiva risoluzione di equazioni di secondo grado di per sé può non essere molto attraente.

In generale, può apparire piuttosto tedioso ciò che può essere acquisito solo con un certo numero di ripetizioni di una pratica 'manipolativa'.[10] Si tratta tuttavia dell'equivalente della tecnica musicale. E non c'è musica senza tecnica. Ed è improprio e fuorviante che qui la storia debba avervi altro ruolo di quello di un eventuale possibile espediente, da usare, comunque, con cautela.

1.3 Il linguaggio da utilizzare

È piuttosto evidente che, anche quando compiamo ogni sforzo per descrivere un'acquisizione matematica nel linguaggio del tempo nel quale è avvenuta, in realtà possiamo solo *avvicinarci* a questo linguaggio attraverso una *mediazione*.

Se, utilizzando la scrittura di Viète, consideriamo l''equazione'

$$B \text{ in } E \text{ adæquabitur } \; A \text{ in } E \text{ bis} + Eq, \tag{1.1}$$

per esprimere ciò che in termini moderni scriveremmo (E indica l'incognita)

$$bx = 2ax + x^2, \tag{1.2}$$

possiamo compiere ogni sforzo ragionevole per 'allontanare' la (1.1) dalla (1.2), ma non c'è alcun modo per rimuovere il nostro patrimonio di conoscenze attuale per immaginare di seguire le argomentazioni di Viète esattamente come uno studioso della fine del Cinquecento.[11]

Di ciò occorre essere consapevoli, e questa consapevolezza implica un confronto serrato e preciso con i *testi*. Si consideri la soluzione abituale

[10] Questo però non significa certo accettare questa pratica in modo acritico. Non riesco per esempio a comprendere perché non possa sostituirsi alla trattazione separata delle equazioni biquadratiche e reciproche l'osservazione che il cambiamento di variabili $x \leftarrow \frac{1-y}{1+y}$ muta un'equazione reciproca in un'equazione avente solo termini di grado pari e viceversa.

[11] Non conosco miglior descrizione (satirica) dell'ingenuità dello storico che presume di 'calarsi nell'epoca di cui tratta' del racconto "Pierre Menard autore del *Chisciotte*" in (Borges 1978).

dell'equazione di secondo grado per 'completamento del quadrato'. Abbiamo, per passi successivi:

$$ax^2 + bx + c = 0. \tag{1.3}$$

Raccogliendo

$$a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = 0, \tag{1.4}$$

ossia, ponendo

$$\frac{b}{a} = p, \quad \frac{c}{a} = q, \tag{1.5}$$

abbiamo

$$x^2 + px + q = 0. \tag{1.6}$$

Ora possiamo procedere, dapprima riscrivendo:

$$x^2 + 2\frac{p}{2}x + q = 0, \tag{1.7}$$

e poi, aggiungendo e togliendo una stessa quantità,

$$x^2 + 2\frac{p}{2}x + \frac{p^2}{4} + q - \frac{p^2}{4} = 0. \tag{1.8}$$

Quindi

$$\left(x + \frac{p}{2}\right)^2 + q - \frac{p^2}{4} = 0. \tag{1.9}$$

Di qui si ottiene, portando a secondo membro e quadrando, la formula risolutiva abituale.

Questo modo di soluzione era noto, si dice, ancor prima di Euclide.

Tuttavia soltanto alla fine del Cinquecento si ha un linguaggio algebrico di forza sufficiente per descrivere le manipolazioni eseguite. Per comprendere questa differenza, vediamo la descrizione di un tipo particolare di soluzione

di equazione di secondo grado in Bombelli, l'autore che chiude la 'grande stagione' degli algebristi italiani del rinascimento.

Vediamo il *Capitolo di Potenze e Tanti eguali a numero.*[12]

Sia data l'equazione di secondo grado

$$ax^2 + bx = c,$$

ove, a, b, c sono quantità positive. L'equazione ha, naturalmente, una sola radice reale positiva. Ecco come il calcolo di questa singola radice(!) viene descritto:

> [1] Partasi ogni cosa per la quantità delle potenze, poi [2] si piglia la metà delli Tanti e si quadra e [3] il produtto si aggionge al numero e [4] della somma e se ne piglia il lato e [5] di detto lato se ne cava la metà delli Tanti, e quello che resterà sarà la valuta del Tanto.

I numeri tra parentesi quadre sono stati introdotti da me per illustrare il procedimento:
[1] corrisponde a sostituire l'equazione originale con

$$x^2 + \frac{b}{a}x = \frac{c}{a}.$$

[2] corrisponde a calcolare

$$\left(\frac{1}{2}\frac{b}{a}\right)^2.$$

[3] dà

$$\left(\frac{1}{2}\frac{b}{a}\right)^2 + \frac{c}{a}.$$

Ora dobbiamo estrarre la radice quadrata ("e se ne piglia il lato"). Dunque ([4]):

$$\sqrt{\left(\frac{1}{2}\frac{b}{a}\right)^2 + \frac{c}{a}}.$$

Finalmente, con [5] abbiamo

$$\sqrt{\left(\frac{1}{2}\frac{b}{a}\right)^2 + \frac{c}{a}} - \frac{b}{2a}. \tag{1.10}$$

[12](Bombelli 1966), p. 190. Riprendo qui quanto ho già esposto in (Galuzzi 1999a).

Bombelli illustra poi il procedimento descritto con un esempio numerico.

Dopo avere esposto un altro modo, corrispondente a scrivere la (1.10) nella forma

$$\frac{\sqrt{\left(\frac{b}{2}\right)^2 + ac} - \frac{b}{2}}{a},$$

ed avere presentato un altro esempio numerico, dimostra poi *geometricamente*, con l'uso di semplici proposizioni contenute negli *Elementi,* la validità delle formule trovate.

Le differenze tra la *formula* risolutiva che si ottiene con la descrizione moderna e la *procedura* proposta da Bombelli,– dimostrata geometricamente,– sono numerose e profonde e noi non abbiamo altra possibilità di quella data dall'interpretare la soluzione di Bombelli a partire dalle nostre conoscenze.

Ecco alcuni spunti di riflessione per l'insegnante:

- Nel primo caso l'algebra è uno strumento dimostrativo, mentre nel secondo la dimostrazione è affidata alla geometria;

- la presentazione algebrica suggerisce in modo ovvio l'esistenza di possibili soluzioni negative, o l'assenza di soluzioni (reali), mentre un problema di geometria elementare non può essere formulato in modo da condurre a soluzioni negative;

- l'insegnate non può 'rimuovere' la sua conoscenza della formula risolutiva per presentare l'argomentazione di Bombelli 'come se' dovesse suggerire la scoperta della soluzione;

- se dovesse presentare ad un allievo la formula risolutiva seguendo Bombelli andrebbe in direzione contraria a quella *economia di pensiero* che è caratteristica del metodo scientifico.

La scelta di presentare la soluzione moderna dell'equazione di secondo grado sembra inevitabile. Ci si può chiedere ora se, accanto a questa presentazione sia utile aggiungere qualche informazione storica. Ora se questa informazione è molto generale e si limita a dire che i babilonesi ancor prima dei greci conoscevano la soluzione, non è di grande profitto. Né lo diviene con l'aggiunta di varî orpelli retorici. Se diviene più specifica, esaminando, per esempio, la soluzione data nel libro secondo degli *Elementi*, la mediazione della quale parlavo all'inizio di questa sezione va posta in modo corretto.

Possiamo, è vero, solo avvicinarci al linguaggio di Euclide, ma lo sforzo per questo avvicinamento va compiuto, per evitare che il risultato euclideo appaia banale.

1.4 Chi non amava la matematica

Benedetto Croce, certamente un grande intellettuale, con pari certezza non amava la matematica:

> La matematica, in quanto matematica, non conosce, ma stabilisce formule di eguaglianza; non serve a conoscere, ma a contare e a calcolare il già conosciuto.
>
> Per contare e calcolare, la matematica ha bisogno di formole, e, per stabilire queste, di certi principi supremi, che si chiamano, a volta a volta, definizioni, assiomi e postulati. Così l'aritmetica ha bisogno della serie numerica la quale, movendo dall'unità, si ottiene aggiungendo sempre un'unità al numero precedente.[13]

Dall'osservazione che ogni numero intero si ottiene dall'unità con un procedere uniforme $(1, 1+1, 1+1+1, \dots)$ Croce traeva la conclusione che tutti i numeri sono fondamentalmente uguali. O meglio, che le loro diversità non possono occupare seriamente i nostri pensieri.

Certamente Benedetto Croce era in grado di cogliere la differenza tra numeri primi e composti e di visualizzare geometricamente questa differenza.

Un numero primo, non può avere una rappresentazione bidimensionale come quella di un numero non primo. Abbiamo, ad esempio

$$12 = 3 \times 4 = \begin{matrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{matrix}$$

Un numero primo non può che rappresentarsi su una linea:

$$7 = \; * \; * \; * \; * \; * \; * \; *$$

Qual è il valore concettuale di questa differenza? Qual è il valore concettuale della esistenza di *infiniti* numeri primi? Assai modesto per Benedetto Croce.

[13]Cfr. (Croce 1909, p. 253).

Per un matematico invece i numeri esibiscono qualità, differenze, strutture che solo una profonda analisi concettuale può cogliere.

Due numeri, come 23 e 29, sarebbero del tutto uguali, secondo Croce. Ma essi sono profondamente diversi per un matematico! Perché possiamo scrivere

$$29 = 25 + 4,$$

ossia 29 è somma di quadrati, mentre, come è facile verificare, non può accadere la stessa cosa per 23. In generale, un numero dispari della forma $4n + 3$ non può essere somma di quadrati.

Ma quali numeri sono somma di quadrati e quali non lo sono? La risposta è tutt'altro che facile[14] e mette in gioco la necessità di analisi profonde della struttura dei numeri interi che vanno ben al di là dello stanco ripetersi dell'aggiunta dell'unità.

Benedetto Croce giudicava il complesso di ricerche come queste, un gioco futile. In generale pensava che la matematica avesse, nelle sue parti più elementari, come in quelle più avanzate, solo un'utilità *pratica*.

Non possiamo rimproverarlo per questo. Possiamo invece addebitargli a colpa grave l'aver edificato un sistema filosofico che ha teorizzato come un valore fondamentale del pensiero ciò che era solo una sua personale valutazione, creando (assieme a Gentile) la mostruosità filosofica delle pseudo-scienze.

Ma possiamo ricavarne la lezione che intelligenza e sottovalutazione della matematica possono coesistere e che non è certo compito della storia della matematica eliminare questa sottovalutazione, che corrisponde ad una sorta di predisposizione individuale. Occorre sempre rammentare che l'intelligenza non ha un'unica forma.

1.5 La 'distanza' dall'insegnamento

Abbiamo sin qui concluso che si può non amare la matematica senza per questo dover essere giudicati privi di capacità intellettive.[15] Abbiamo illu-

---

[14]Sia n un intero positivo, e poniamo $n = b^2c$. Allora n si può scrivere come somma di due quadrati se e solo se nessun numero primo della forma $4k + 3$ divide c. Si veda (**?**, p. 164).

[15]Ma credo d'aver chiarito che non amare la matematica non implica che si debba esibire con stupido compiacimento la propria incapacità di comprenderla. Né soprattutto che si debba poi lasciare intendere che il fastidio per la sua (presunta) banalità sia la necessaria premessa per cogliere i più alti valori dello spirito.

strato il punto di vista secondo il quale l'uso della storia non va inteso come un modo accattivante e giocoso per rendere attraente una disciplina che, se attrae, attrae di per sé. Abbiamo chiarito che un eventuale uso della storia nella didattica deve avvenire mediante un confronto con i testi. Rimane un ultimo punto: ammesso che la conoscenza storica sia, per il docente, un potente stimolo per una didattica personale e profonda, e possa essere per lo studente un modo di penetrare ancora più a fondo nella conoscenza della disciplina, quanto 'vicina' deve essere la conoscenza storica alla pratica didattica?

Quali testi occorre conoscere per insegnare la geometria elementare? Gli *Elementi*? Le *Grundlagen* di Hilbert? Le ricerche di Emil Artin sul problema della coordinatizzazione?

A prima vista sembra evidente che la scelta debba cadere su ciò che è più vicino alla pratica didattica... O su ciò che l'uso ha consacrato.

Tuttavia una riflessione più attenta mostra che le connessioni possono essere meno evidenti.

Si supponga d'avere il problema di dover insegnare l'ortografia e la sintassi italiana. Quali conoscenze occorre possedere e quali testi della nostra letteratura occorre aver letto?

Non sembra che Pirandello sia tra i primi autori che occorra considerare.[16] Ma si considerino queste frasi, tratte in ordine sparso, dalle novelle *Padron Dio* e *La casa dell'agonia* della raccolta *Una giornata*:

> *Sdrajato* per terra, s'immergeva in quel silenzio [...]
>
> Se questo fosse finalmente sopravvenuto, *lui* ne avrebbe provato dispiacere [...]
>
> Sul rettangolo azzurro della finestra spiccava un vaso di *geranii* rossi [...]

Pirandello era un profondo conoscitore della lingua italiana.[17] Aveva anche scritto importanti contributi teorici sulla lingua. Sceglie 'lui' e 'lei'

[16]Naturalmente non intendo qui esprimere un parere autorevole sulla lingua italiana. Intendo invece sottolineare il fatto che, accanto ai riferimenti consueti ai 'padri' della lingua, Petrarca, Dante, Manzoni, ecc. si trovano anche altri autori ai quali è utile e stimolante riferirsi. Naturalmente Pirandello era un profondo conoscitore della lingua italiana (si veda, per esempio, l'*Appendice* di Simona Costa a (Pirandello 1993)). Ma il riferimento a Pirandello non è tra i più diffusi nell'insegnamento della sintassi italiana.

[17]Si veda la nota 16.

come soggetto perché giudica ‘egli’ ed ‘ella’ forme troppo letterarie. Preferisce che la ‘i’ intervocalica si trasformi in ‘j’. Preferisce ‘geranii’ a ‘geranî’ od a ‘gerani’.

L’importanza che le sue *Novelle per un anno* hanno avuta,- e continueranno ad avere,- nella cultura italiana dimostra con chiara evidenza l’importanza di una scelta linguistica che ponga la lingua letteraria a breve distanza dal parlare comune. Le scelte di ‘j’ ed ‘ii’ non hanno invece avuto largo seguito.

Non dobbiamo trarne la conclusione che ci vuole molta cautela nel proporre degli usi grammaticali che allontanino dalla lingua parlata (egli, ella)? O che, simmetricamente, è difficile introdurre ciò che la pratica della lingua corrente va semplificando (la j intervocalica, la doppia i)?

Andrea Camilleri, nella Nota *Mani avanti*, apposta al romanzo *Il corso delle cose*, spiega le ragioni del suo ‘linguaggio’ personale. Le sue scelte linguistiche si riconnettono idealmente alle ragioni che spingevano Pirandello (autore per altro che gli è estremamente familiare) a prediligere ‘lui’ e ‘lei’. E va anche oltre trasponendo termini dalla parlata siciliana che stanno divenendo familiari a molti lettori.[18]

Quanto la lettura di Pirandello, od anche di Camilleri, può essere di profitto a chi vuole ‘insegnare’ l’uso corretto della lingua italiana? La risposta mi pare ovvia. Come è ovvio che la lettura d’un testo da riconnettersi immediatamente alla pratica didattica quotidiana non sia il modo migliore per conferire a questa pratica sostanza e dignità.[19]

[18] Si veda la premessa al Glossario posta in appendice di (Camilleri 2000).

[19] Ovviamente non è in discussione il mutare della lingua sul lungo periodo (il latino e le lingue romanze...). Né, in generale, il mutare della lingua anche su periodi più brevi (San Paolo non usa più l’ottativo nella lingua greca; il passato remoto tende a sparire dall’uso corrente della lingua italiana ...). Ciò che voglio sottolineare è come *in uno stesso periodo*, quando le strutture essenziali sembrano ben codificate, la lettura degli *autori* può offrire prospettive assai ricche.

Capitolo 2

Frazioni continue

2.1 Premessa

Lo scopo di queste lezioni è quello di presentare alcune semplici proprietà delle frazioni continue. Nella parte finale vedremo uno dei primi risultati ottenuti da Evariste Galois.

Galois è, nella storia della matematica, l'eroe romantico per eccellenza. Proprio per questa ragione, la possibilità di parlare di Galois può essere un'ottima occasione per attirare l'attenzione degli studenti e per un loro coinvolgimento attivo. Al tempo stesso, bisogna evitare che la presentazione si risolva in pura ideologia e che le vicende biografiche siano la premessa per affermazioni generiche del tipo 'Galois è il fondatore dell'algebra moderna', 'Galois è l'inventore della teoria dei gruppi', ecc. Senza che a queste affermazioni faccia seguito una presentazione, ancorché minimale, dei suoi contributi scientifici.[1] Ovviamente, non è possibile presentare la *Teoria di Galois* senza un'adeguata premessa algebrica (che, in genere, non fa parte del bagaglio scientifico d'uno studente della scuola superiore). È però possibile presentare il suo risultato sulle frazioni continue. Certamente questo risultato non è paragonabile per importanza ai suoi profondi teoremi algebrici. Si tratta però, comunque, di un lavoro notevole.

[1]Comunque, la presentazione più equilibrata, a mio giudizio, delle vicende biografiche di Galois è (Rothman 1982). Interessante, anche se molto fantasioso, è (Toti Rigatelli 1996). Il romanzo di Petsinis (Petsinis 1997), tradotto anche in italiano, è di gradevole lettura anche se la matematica attribuita a Galois è inadeguata.

2.2 Qualche osservazione sui numeri

La scoperta dell'esistenza di quantità geometriche non esprimibili mediante rapporti di numeri interi risale ai pitagorici.

Ecco un modo per dimostrare l'irrazionalità di $\sqrt{2}$.[2] Procediamo per assurdo: sia:

$$\sqrt{2} = \frac{m}{n}, \quad \text{ossia,} \tag{2.1}$$

$$2n^2 = m^2. \tag{2.2}$$

Il numero m deve essere pari: $m = 2m_1$.

$$2n^2 = 4m_1^2. \tag{2.3}$$

Anche n deve essere pari: $n = 2n_1$.

$$\frac{m}{n} = \frac{2m_1}{2n_1} = \frac{m_1}{n_1}. \tag{2.4}$$

Il procedimento può continuare all'infinito?

$$\frac{m}{n} = \frac{\frac{m}{2}}{\frac{n}{2}} = \frac{\frac{m}{4}}{\frac{n}{4}} = \dots$$

In tal caso dovremmo accettare l'esistenza di numeri *interi* che possano continuamente essere dimezzati. Questa è la conclusione assurda alla quale si perviene.[3]

La tradizione vuole che i pitagorici ricercassero l'ordine e l'armonia dell'universo nella semplicità dei rapporti tra numeri interi.[4] La scoperta degli irrazionali avrebbe così prodotto la crisi della scuola pitagorica.

---

[2] Più esattamente bisognerebbe dire la incommensurabilità della diagonale di un quadrato scegliendo il lato come misura.

[3] Naturalmente si può arrivare ad una conclusione parimenti assurda assumendo l'unicità della decomposizione in fattori primi. Ma questa richiesta è eccessiva, e traspone l'argomentazione pitagorica in un contesto troppo sofisticato. La letteratura sull'argomento è molto ampia. Mi limito a segnalare (Knorr 1975; Stillwell 2002).

[4] Sempre alla scuola pitagorica si attribuisce la scoperta del fatto che rapporti semplici tra le lunghezze delle corde $\frac{1}{2}, \frac{3}{2}, \frac{4}{3} \dots$ corrispondono agli intervalli musicali semplici: l'ottava, la quinta, la quarta. Si veda, per esempio, (Ferreira 2002).

La questione dell'effettiva portata di questa crisi (o perfino della sua esistenza) è molto controversa. Occorre però evitare di suggerire l'idea che esista una radicale separazione tra numeri razionali ed irrazionali non suscettibile di ulteriore indagine e che gli irrazionali, tutti, siano accomunati da una assoluta ed indifferenziata complessità algoritmica che li contrappone irrimediabilmente ai numeri razionali.

L'algoritmo delle frazioni continue mostra invece che gli irrazionali quadratici reali (le soluzioni reali delle equazioni di secondo grado a coefficienti interi) possiedono una semplicità di calcolo non dissimile da quella dei numeri frazionari.

2.2.1 Radici quadrate: algoritmi

Consideriamo l'algoritmo per estrarre la radice quadrata. Esso si fonda sulla seguente proprietà che può essere utilizzata per un calcolo ricorsivo.

$$
\begin{aligned}
&(x_1 + x_2)^2 = x_1^2 + (2x_1 + x_2)x_2 \\
&(x_1 + x_2 + x_3)^2 = (x_1 + x_2)^2 + (2x_1 + 2x_2 + x_3)x_3 \\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
&(x_1 + \cdots + x_{n-1} + x_n)^2 = (x_1 + \cdots + x_{n-1})^2 + (2x_1 + \cdots + 2x_{n-1} + x_n)x_n
\end{aligned}
$$

Questa semplice proprietà è alla base del calcolo aritmetico abituale. Ad esempio, per calcolare $\sqrt{2}$ dobbiamo dapprima individuare il più grande intero x_1 per il quale sia

$$x_1^2 < 2.$$

Dunque $x_1 = 1 = \frac{10}{10}$

Poi si tratta di individuare il più grande intero x_2 tale che

$$(20 + x_2)x_2 < 100,$$

il che dà $x_2 = 4 = \frac{40}{100}$. Ora occorre calcolare x_3 in modo che

$$(240 + x_3)x_3$$

non superi 400 e si ottiene $x_3 = 1, \dots$

Il calcolo procede con sempre maggior complessità, ed occorre utilizzare tutto quanto trovato in precedenza. Per calcolare la cifra successiva, occorre determinare il più grande intero x_4 tale che

$$(2820 + x_4)x_4 < 11900, \text{ ecc.}$$

Si consideri invece lo schema di calcolo seguente per $\sqrt{2}$ (che verrà giustificato in seguito):

$$
\begin{aligned}
&p{-}1 = 1, q_{-1} = 0;\\
&p_0 = \mathbf{1}, q_1 = 1;\\
&p_{k+1} = \mathbf{2} \cdot p_k + p_{k-1}; && (2.5)\\
&q_{k+1} = \mathbf{2} \cdot q_k + q_{k-1}. && (2.6)
\end{aligned}
$$

Consideriamo (per $k \geq 0$) le frazioni

$$\frac{p_k}{q_k}.$$

Si ha facilmente:

$$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \frac{239}{169}, \ldots$$

Si osservi ora che:

- Il calcolo è molto semplice;
- le frazioni approssimano molto rapidamente $\sqrt{2}$;
- Non occorre, ad ogni passo 'ricapitolare' tutto il procedimento;
- Ciò che di **specifico** compare di $\sqrt{2}$ è solo la **parte intera** 1, ed il 'periodo', 2.

Con $\sqrt{5}$ il calcolo procede in modo molto simile, occorre però porre $a_0 = 2$ e modificare le (5),(6), ponendo

$$
\begin{aligned}
p_{k+1} &= \mathbf{4} \cdot p_k + p_{k-1};\\
q_{k+1} &= \mathbf{4} \cdot q_k + q_{k-1}.
\end{aligned}
$$

Abbiamo

$$\frac{2}{1}, \frac{9}{4}, \frac{38}{17}, \frac{161}{72}, \frac{682}{305}, \ldots$$

Il tipo di calcolo che abbiamo visto per $\sqrt{2}, \sqrt{5}$ si estende ad ogni numero della forma $\sqrt{n}$ con questo schema più generale:

$$
\begin{aligned}
&p_{-1} = 1, p_{-1} = 0;\\
&p_0 = c_0, q_1 = 1;\\
&p_{k+1} = c_{k+1} p_k + p_{k-1}; && (2.7)\\
&q_{k+1} = c_{k+1} q_k + q_{k-1},
\end{aligned}
$$

dove $c_0 = \lfloor \sqrt{n} \rfloor$ e i numeri c_k non sono più necessariamente tutti uguali, ma si ripetono da un certo posto in poi (su questo otterremo un risultato più preciso nella Sezione 2.4.3). Ad esempio, per $\sqrt{19}$, abbiamo per i successivi c_k

$$4, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, \dots$$

Possiamo scrivere, per indicare l'algoritmo:

$$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}\,]$$

È possibile che questo tipo di calcolo per gli irrazionali quadratici abbia preceduto la teoria delle proporzioni di tradizionalmente attribuita ad Eudosso.[5] È un calcolo tuttavia, molto particolare. È molto facile calcolare il reciproco di un numero: se $\gamma = [c_0, c_1, c_2, \dots]$ è un numero positivo ($c_0 \geq 0$),

$$\gamma^{-1} = [0, c_0, c_1, c_2, \dots]$$

Ma non esiste alcun algoritmo semplice per la somma!

Ad esempio:

$$\sqrt{2} = [1, \overline{2}\,], \quad \sqrt{5} = [2, \overline{4}\,]$$

Ma

$$\sqrt{2} + \sqrt{5} = [3, 1, 1, 1, 6, 8, 1, 2, 1, 2, 2, 1, 101, 13, 1 \dots]$$

Fino ad ora non è stata notata alcuna regolarità.

2.3 Principali proprietà delle frazioni continue

Ad Eulero si deve prima esposizione sistematica della teoria delle frazioni continue.[6] La teoria è stata ripresa e sviluppata poi Lagrange nelle note aggiunte alla traduzione francese dell'algebra di Eulero.[7]

---

[5] Si vedano, in particolare, i molti lavori di Fowler. Tra questi, in particolare, (Fowler 1987). Una rapida esposizione della teoria di Eudosso si trova in (Galuzzi and Rovelli 1997).

[6] Nella *Introductio in analysin infinitorum*, del 1748. Si può vedere la facilmente accessibile traduzione inglese: (Euler 1988, cap. XVIII).

[7] Si tratta di (Euler 1773). Si veda anche (Lagrange 1879, vol. VII).

Un primo aspetto con il quale compaiono naturalmente le frazioni continue è quello della ricerca di frazioni 'più semplici'.[8] Data la frazione

$$\frac{345723}{245125} = 1.410394697,$$

abbiamo

$$\frac{24}{17} = 1.411764706, \quad \frac{55}{39} = 1.410256410 \tag{2.8}$$

Queste frazioni semplici si trovano (come vedremo) mediante lo sviluppo in frazione continua.

L'algoritmo di Euclide si lega naturalmente alle frazioni continue *finite*. Si tratta di un altro modo, conveniente, di rappresentare i numeri razionali. Consideriamo la frazione $\frac{137}{101}$.

$$\begin{aligned} 137 &= \mathbf{1} \cdot 101 + 36 \\ 101 &= \mathbf{2} \cdot 36 + 29 \\ 36 &= \mathbf{1} \cdot 29 + 7 \\ 29 &= \mathbf{4} \cdot 7 + 1 \end{aligned}$$

Allora, dalla prima riga:

$$\frac{137}{101} = \mathbf{1} + \frac{36}{101} = 1 + \frac{1}{\frac{101}{36}}.$$

Dalla seconda riga:

$$\frac{137}{101} = 1 + \cfrac{1}{\mathbf{2} + \cfrac{29}{36}} = 1 + \cfrac{1}{2 + \cfrac{1}{\cfrac{36}{29}}}$$

Con i numeri trovati: $1, 2, 1, 4$ possiamo costruire la **frazione continua**:

$$\mathbf{1} + \cfrac{1}{\mathbf{2} + \cfrac{1}{\mathbf{1} + \cfrac{1}{\mathbf{4}}}}$$

---

[8] Una chiara concisa e rigorosa presentazione degli aspetti essenziali della teoria delle frazioni continue è (Bombieri and van der Poorten 1995).

Si può vedere anche il classico (Hardy and Wright 1971) o i più recenti (Lorentzen and Waadeland 1992; Rockett and Szüs 1992). (Olds 1968) è un testo elementare ma ben fatto.

Le frazioni più semplici sono quelle che si ottengono usando solo 'una parte' della lista
$$[1, 2, 1, 4].$$
In questo modo sono stae ottenute le frazioni (2.8).

Ecco un altro esempio: l'algoritmo per $\sqrt{2}$:
$$(\sqrt{2}-1)(\sqrt{2}+1) = 1.$$
Allora (!)
$$\sqrt{2}-1 = \frac{1}{\sqrt{2}+1} = \frac{1}{\sqrt{2}-1+2}$$
Quindi
$$\sqrt{2}-1 = \cfrac{1}{2+\cfrac{1}{\sqrt{2}+1}}$$
Si può procedere indefinitamente: otteniamo la **frazione continua infinita**
$$1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\dots}}}.$$
DEFINIZIONE 1. – Una frazione continua (aritmetica) finita è
$$c_0+\cfrac{1}{c_1+\cfrac{1}{c_2+\ddots+\cfrac{1}{c_h}}}, \quad (c_i \geq 1 \text{ per } i \geq 1).$$
Evidentemente è solo un altro modo (vantaggioso) di scrivere un numero razionale.

DEFINIZIONE 2. – Le successive frazioni
$$\frac{p_0}{q_0} = c_0,\ \frac{p_1}{q_1} = c_0+\frac{1}{c_1},\ \frac{p_2}{q_2} = c_0+\cfrac{1}{c_1+\cfrac{1}{c_2}}, \dots$$
sono dette *convergenti.* I numeri c_i sono detti *quozienti parziali.*

Mostriamo ora che p_k, q_k verificano le formule seguenti (ove, per comodità, si introducono anche p_{-1} e q_{-1}):

$$\begin{aligned}
&p_{-1} = 1, p_0 = c_0,\\
&p_{k+1} = c_{k+1} \cdot p_k + p_{k-1}\\
&q_{-1} = 0, q_0 = 1,\\
&q_{k+1} = c_{k+1} \cdot q_k + q_{k-1}.
\end{aligned} \tag{2.9}$$

Sia $\dfrac{p_k}{q_k}$ la k-esima convergente. Esaminiamo il passaggio alla convergente successiva: si tratta di effettuare la sostituzione

$$a_{k+1} \longleftarrow c_{k+1} + \frac{1}{c_{k+2}}.$$

Allora:

$$\frac{\left(c_{k+1} + \frac{1}{c_{k+2}}\right) p_k + p_{k-1}}{\left(c_{k+1} + \frac{1}{c_{k+2}}\right) q_k + q_{k-1}} = \frac{p_{k+1} + \frac{p_k}{c_{k+2}}}{q_{k+1} + \frac{q_k}{c_{k+2}}} = \frac{c_{k+2}p_{k+1} + p_k}{c_{k+2}q_{k+1} + q_k}$$

Abbiamo verificato le (2.9).

Osservazione 1. – Si noti che possiamo scrivere:

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} \begin{pmatrix} c_{k+1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c_{k+1}p_k + p_{k-1} & p_k \\ c_{k+1}q_k + q_{k-1} & q_k \end{pmatrix},$$

e quindi

$$\begin{pmatrix} c_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_{k+1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_{k+1} & p_k \\ q_{k+1} & q_k \end{pmatrix}. \tag{2.10}$$

Ne segue che

$$p_{k+1}q_k - p_k q_{k+1} = (-1)^k.$$

Corollario 1. – Le frazioni $\dfrac{p_k}{q_k}$ date dalle (2.9) sono ridotte ai minimi termini.

Corollario 2. – Trasponendo il prodotto matriciale (2.10), abbiamo

$$\frac{p_k}{p_{k-1}} = [c_k, c_{k-1}, \ldots, c_0], \ \frac{q_k}{q_{k-1}} = [c_k, c_{k-1}, \ldots, c_1].$$

2.3.1 Un'equazione diofantea

Una semplice applicazione: risolviamo, quando possibile, l'equazione

$$mx + ny = 1.$$

Supponiamo m, n primi fra loro, e sviluppiamo in frazione continua.

$$\frac{m}{n} = \frac{p_{k+1}}{q_{k+1}}.$$

Abbiamo

$$mq_k - p_k n = (-1)^k.$$

Esempio 1. – Risolviamo

$$27x + 43y = 1.$$

Abbiamo

$$\frac{27}{43} = \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{5}}}}}$$

La penultima ridotta vale $\frac{5}{8}$. Allora

$$27 \cdot 8 - 43 \cdot 5 = 1. \quad \square$$

Osservazione 2. – Da

$$p_{k+1}q_k - p_k q_{k+1} = (-1)^k,$$

deduciamo

$$\left|\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right| = \frac{1}{q_{k+1}q_k}.$$

Consideriamo la differenza

$$\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k q_{k+1}}.$$

Poiché, come abbiamo visto

$$q_{-1} = 0, q_0 = 1, \quad q_{k+1} = a_{k+1} \cdot q_k + q_{k-1},$$

$q_1 \geq 1, q_2 \geq 2, \dots$ e, in generale, $q_k \geq f_k$, ove f_k è il k-esimo numero di Fibonacci.

2.3.2 La convergenza

Abbiamo

$$\frac{p_{k+1}}{q_{k+1}} = \frac{p_0}{q_0} + \sum_{i=0}^{k} \left(\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} \right) = \frac{p_0}{q_0} + \sum_{i=0}^{k} \frac{(-1)^i}{q_i q_{i+1}}.$$

La serie (a segni alternati)

$$\sum_{i=0}^{\infty} \frac{(-1)^i}{q_i q_{i+1}}$$

è convergente, e quindi il limite

$$\gamma = \lim_{k\to\infty} \frac{p_k}{q_k}$$

esiste. La convergenza avviene alternatamente dal di sotto e dal di sopra.

Esempio 2. – Consideriamo ancora la frazione continua

$$[1, 2, 2, 2, \dots]$$

Abbiamo

$$p : 1, 1, 1 \cdot 2 + 1 = 3, 3 \cdot 2 + 1 = 7, 7 \cdot 2 + 3 = 17, \dots$$
$$q : 0, 1, 1 \cdot 2 + 0 = 2, 2 \cdot 2 + 1 = 5, 5 \cdot 2 + 2 = 12, \dots$$

Quindi, le convergenti sono

$$1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \dots$$

Abbiamo

$$1, 1.5, 1.4, 1.416666\dots,$$

procedendo nel calcolo si ha

$$\frac{41}{29}, \frac{99}{70} = 1.414285714.$$

Si ottengono approssimazioni molto buone. Su questo si veda la Sezione 2.3.3.

Abbiamo già osservato (cfr. pag. 25) che le frazioni continue *finite*

$$\frac{p_h}{q_h} = [c_0, c_1, \dots, c_h]$$

sono dette le convergenti del numero reale γ definito dalla frazione continua.

DEFINIZIONE 3. – Le *code*

$$\gamma_{h+1} = [c_{h+1}, c_{h+2}, \ldots]$$

sono dette *quozienti completi*.

Formalmente, possiamo scrivere

$$\gamma = [c_0, c_1, \ldots, c_h, \gamma_{h+1}].$$

Abbiamo

$$\gamma - \frac{p_h}{q_h} = (-1)^h \left[\frac{1}{q_h q_{h+1}} - \frac{1}{q_{h+1} q_{h+2}} + \ldots \right].$$

Ne consegue che

$$\left| \gamma - \frac{p_h}{q_h} \right| < \frac{1}{q_h q_{h+1}}.$$

Osservando che $q_{h+1} = c_{h+1} q_h + q_{h-1}$ si ha anche

$$\left| \gamma - \frac{p_h}{q_h} \right| < \frac{1}{c_{h+1} q_h^2}.$$

Se dunque si ha un *quoziente parziale* c_{h+1} molto grande si ha una buona approssimazione.

Osserviamo ora che

$$\gamma = [c_0, c_1, \ldots] = c_0 + \frac{1}{[c_1, c_2, \ldots]}$$

e dunque

$$c_0 = \lfloor \gamma \rfloor \quad \text{e} \quad \gamma_1 = [c_1, c_2, \ldots] = (\gamma - c_0)^{-1}.$$

Avremo, in generale

$$c_h = \lfloor \gamma_h \rfloor \quad \text{e} \quad \gamma_{h+1} = (\gamma_h - c_h)^{-1}.$$

ESEMPIO 3. – Rivediamo lo sviluppo in frazione continua di $\sqrt{2}$. Abbiamo

$$c_0 = \left\lfloor \sqrt{2} \right\rfloor = 1$$

e

$$\gamma_1 = \left(\sqrt{2} - 1 \right)^{-1} = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{2 - 1} = \sqrt{2} + 1.$$

Allora

$$c_1 = \lfloor \gamma_1 \rfloor = 2$$

mentre

$$\gamma_2 = \left[\left(\sqrt{2}+1\right) - 2\right]^{-1} = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1.$$

Dunque

$$\sqrt{2} = [1, 2, 2, 2, \ldots].$$

Esempio 4. – Osserviamo che

$$\frac{\sqrt{5}-1}{2} = \cfrac{1}{1+\cfrac{\sqrt{5}-1}{2}}$$

e dunque

$$1 + \frac{\sqrt{5}-1}{2} = \frac{\sqrt{5}+1}{2} = [1, 1, 1, \ldots].$$

Il più 'semplice' sviluppo in frazione continua corrisponde alla *parte aurea*.[9]

2.3.3 Qualche approfondimento

Definizione 4. – Sia ξ un numero reale. Diremo che $\frac{p}{q}$ è una **migliore approssimazione razionale** di ξ se e solo se per ogni altra frazione $\frac{r}{s}$ con $s > 0$ la disuguaglianza

$$\left|\xi - \frac{r}{s}\right| < \left|\xi - \frac{p}{q}\right|$$

implica $s > q$.

Teorema 1. – Le convergenti di una frazione continua aritmetica, di ordine maggiore od uguale ad 1, relative ad un numero reale ξ, sono migliori approssimazioni.

Dimostrazione. Vediamo un Lemma preliminare.

Lemma 1. – $\xi, \frac{p_n}{q_n}, \ldots$ Sia $\frac{r}{s} \neq \frac{p_n}{q_n}$ con $0 < s < q_n$. Allora

$$|s\xi - r| \geq |q_{n-1}\xi - p_{n-1}| > |q_n\xi - p_n|.$$

[9] Sulla sezione aurea, si veda (Scimone 1997).

Dimostrazione. Esistono due numeri *interi* x, y tali che

$$\begin{cases} p_n\, x + p_{n-1} y = r \\ q_n\, x + q_{n-1} y = s. \end{cases}$$

(La matrice ha determinante ± 1.) Non può essere $y = 0 \ldots$ Per ipotesi $s < q_n$ e quindi o $x = 0$ oppure x e y sono di segno opposto. Consideriamo l'identità

$$s\xi - r = x(q_n \xi - p_n) + y(q_{n-1}\xi - p_{n-1}).$$

Le due quantità entro parentesi hanno segno opposto (le convergenti sono alternatamente maggiori e minori di ξ) ed anche x e y hanno segno opposto. Allora

$$|s\xi - r| = |x(q_n \xi - p_n)| + |y(q_{n-1}\xi - p_{n-1})|$$

Poiché $y \neq 0$, abbiamo

$$|s\xi - r| \geq |q_{n-1}\xi - p_{n-1}|.$$

Si ha sempre

$$|q_n \xi - p_n| < |q_{n-1}\xi - p_{n-1}|.$$

Dimostrazione (del Teorema)– ξ, $\frac{p_n}{q_n}$. Sia $\frac{r}{s} \neq \frac{p_n}{q_n}$ una frazione che verifica

$$\left|\xi - \frac{r}{s}\right| \leq \left|\xi - \frac{p_n}{q_n}\right|$$

con $0 < s < q_n$. Allora moltiplicano il primo membro per s ed il secondo per q_n, abbiamo

$$|s\xi - r| \leq |q_n \xi - p_n|$$

in contraddizione con il Lemma. $\square$

2.4 Il metodo di Lagrange

Il polinomio $f(x) = f_0(x)$, di grado n, abbia un'unica radice positiva γ, e sia

$$\lfloor \gamma \rfloor = c_0.^{10}$$

[10] In realtà è sufficiente supporre che tra c_0 e $c_0 + 1$ cada un'unica radice. I riferimenti bibliografici ed un'esposizione del fatto che il metodo di Lagrange, attraverso l'uso del teorema di Vincent, conduce anche autonomamente alla *separazione* delle radici sono dati in (Alesina and Galuzzi 1998).

Il nuovo polinomio

$$f_1(x) = \pm x^n f_0\left(c_0 + \frac{1}{x}\right)$$

ha un'unica radice maggiore di 1, perché la trasformazione

$$x \leftarrow c_0 + \frac{1}{x}$$

fornisce la corrispondenza biunivoca

$$(c_0, c_0 + 1) \rightleftarrows (\infty, 1).$$

Sia c_1 la parte intera della radice positiva di $f_1(x)$. Si ponga:

$$f_2(x) = \pm x^n f_1\left(c_1 + \frac{1}{x}\right)$$

Evidentemente, procedendo nello stesso modo, si ottiene la radice espressa come frazione continua:

$$\gamma = [c_0, c_1, c_2, \dots].$$

Il metodo di approssimazione di Lagrange è dunque intrinsecamente legato alle frazioni continue.

Esempio 5. – Sia $f_0(x) = x^2 - 2, c_0 = 1$. Allora

$$f_1(x) = -x^2\left(\left(1 + \frac{1}{x}\right)^2 - 2\right) = x^2 - 2x - 1.$$

La parte intera della radice di $f_1(x)$ è 2.

$$\begin{aligned} f_2(x) &= -x^2\left(\left(2 + \frac{1}{x}\right)^2 - 2\left(2 + \frac{1}{x}\right) - 1\right) = \\ &= x^2 - 2x - 1 = f_1(x) \end{aligned}$$

Allora, ancora una volta:

$$\sqrt{2} = [1, 2, 2, 2, \dots].$$

Esercizio 1. – Determinare lo sviluppo in frazione continua della soluzione positiva di

$$x^2 - (n^2 + 1) = 0, \quad n \in \mathbb{N}$$

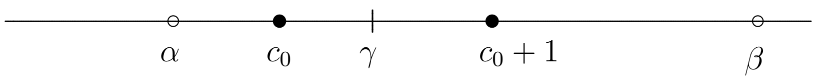
e della soluzione positiva di

$$x^2 - (n^2 - 1) = 0, \quad n \in \mathbb{N}.$$

Se il polinomio $f_0(x)$ ha una sola radice γ con parte intera $\lfloor c_0 \rfloor$, dopo il primo passaggio si un polinomio che ha una sola radice positiva e maggiore di 1. Sia

$$f(x) = (x - \gamma)(x - \alpha)(x - \beta) \cdots$$

e supponiamo che due radici reali α, β siano disposte come in figura.



Con il metodi di Lagrange otteniamo il polinomio

$$f_1(x) = [(c_0 - \gamma)x + 1][(c_0 - \alpha)x + 1][(c_0 - \beta)x + 1] \cdots$$

Ora

$$\frac{1}{\gamma - c_0} > 1, \quad \frac{1}{\alpha - c_0} < 0, \quad 0 < \frac{1}{\beta - c_0} < 1.$$

Dopo due passaggi otteniamo un polinomio con una sola radice positiva.

Esempio 6. – Il polinomio

$$f_0(x) = x^3 - 10x^2 + 31x - 29$$

ha le radici (approssimate)

$$1.753, 3.445, 4.801.$$

Il calcolo di $f_1(x)$ dà

$$x^3 + 2x^2 - x + 1,$$

il quale ha le radici

$$-0.801, 0.554, 2.246.$$

Quindi

$$f_2(x) = x^3 - 3\,x^2 - 4\,x - 1$$

il quale ha le radici

$$-0.692, -0.356, 4.048.$$

$$3 + \cfrac{1}{2 + \cfrac{1}{4}} = \frac{31}{9} = 3.\overline{4}.$$

2.4.1 Il teorema di Lagrange sugli irrazionali quadratici

Consideriamo una frazione continua *puramente periodica*:

$$\gamma = [\overline{c_0, c_1, \ldots, c_n}].$$

Mostriamo che γ è radice di un'equazione di secondo grado.
Sia, per semplicità,[11]

$$\gamma = [\overline{a, b, c}].$$

Allora

$$\gamma = a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{\gamma}}}.$$

Quindi

$$\gamma = \frac{A + B\gamma}{C + D\gamma}.$$

Supponiamo ora che vi sia un anti-periodo:

$$\gamma = [a, b, \overline{c, d, e}].$$

Quindi

$$\gamma - a = \cfrac{1}{b + \cfrac{1}{[\overline{c, d, e}]}},$$

$$\frac{1}{\gamma - a} = b + \frac{1}{[\overline{c, d, e}]},$$

[11]Le dimostrazioni seguenti sono condotte su esempi 'paradigmatici' come spesso nella matematica tra fine Settecento e metà dell'ottocento. Ma non si incontra alcuna difficoltà nel riproporle in linguaggio moderno.

$$\Gamma = \cfrac{1}{-b + \cfrac{1}{\gamma - a}} = [\overline{c, d, e}].$$

Allora Γ è radice di un'equazione di secondo grado. È chiaro che, con una semplice sostituzione,ancora si ottiene che γ è radice di un'equazione di secondo grado

ESEMPIO 7. – $\gamma = [1, 2, \overline{3}]$. Allora

$$\frac{1}{\gamma - 1} = 2 + \frac{1}{[\overline{3}]}, \; \frac{\gamma - 1}{3 - 2\gamma} = [\overline{3}] = \Gamma.$$

Allora

$$\Gamma^2 - 3\Gamma - 1 = 0$$

e quindi

$$3\gamma^2 - 5\gamma + 1 = 0$$

Quindi

$$\frac{5}{6} + \frac{1}{6}\sqrt{13} = [1, 2, \overline{3}]. \quad \square$$

OSSERVAZIONE 3. – Dato il polinomio di secondo grado[12]

$$f_0(x) = a_0x^2 + b_0x + c_0$$

una qualsiasi trasformazione della forma

$$x \longleftarrow n_0 + \frac{1}{x}$$

lascia invariato il discriminante.[13]

Si ha infatti il nuovo polinomio

$$(a_0n_0^2 + b_0n_0 + c_0)x^2 + (b_0 + 2a_0n_0)x + a_0.$$

Il calcolo diretto da:

$$(b_0 + 2a_0n_0)^2 - 4a_0(a_0n_0^2 + b_0n_0 + c_0) = b_0^2 - 4a_0c_0.$$

[12]Nell'esposizione seguente tengo conto di (Ballieu 1942).

[13]Il risultato è evidente se pensiamo la trasformazione in due passi: una traslazione seguita dal passaggio all'equazione reciproca.

Sia ora $f_0(x)$ un polinomio di secondo grado irriducibile avente radici reali γ, δ con parte intera *diversa*.

$$\gamma \in (c_0, c_0+1), \delta \notin (c_0, c_0+1).$$

Dopo al più due passaggi (con il metodo di Lagrange) abbiamo un polinomio con una radice *positiva* (e maggiore di 1) ed una *negativa*.[14] Questo significa che il coefficiente del termine di grado 0 deve essere negativo (supponendo, naturalmente che il primo coefficiente sia positivo).
Quindi, nell'ipotesi $\delta > \gamma$, avremo

$$f_2(x) = a_2x^2 + b_2x + c_2, \text{ con } c_2 < 0.$$

Sia ora

$$f_h(x) = a_hx^2 + b_hx + c_h, \text{ con } a_hc_h < 0, \ b_h^2 - 4a_hc_h > 0.$$

Allora anche $f_{h+1}(x)$ ha la stessa proprietà.

Scriviamo $f_h(x)$ in modo da porre in evidenza il fatto che ha radici reali di segno opposto:

$$f_h(x) = a_h(x-\alpha)(x+\beta), \text{ con } \alpha, \beta > 0.$$

Se $n_a = \lfloor \alpha \rfloor$, il polinomio $f_{h+1}(x)$ ha le radici

$$\frac{1}{\alpha - n_a}, -\frac{1}{\beta + n_a}.$$

Abbiamo ancora radici di segno opposto, il che implica $a_{h+1}c_{h+1} < 0$.

Fissato il valore del discriminate

$$\Delta = b_h^2 - 4a_hc_h,$$

se

$$a_hc_h < 0$$

abbiamo solo un **numero finito** di polinomi con discriminante Δ.

Nell'ipotesi di radici γ, δ con parte intera diversa, dopo un numero finito di trasformazioni del metodo di Lagrange dobbiamo ritrovare lo stesso polinomio.

[14] Si noti che la radice negativa, con una ulteriore trasformazione del procedimento di Lagrange, viene trasformata in una radice ancora negativa ma di modulo inferiore all'unità.

Sia ora $\lfloor \gamma \rfloor = \lfloor \delta \rfloor$ e siano

$$\gamma_1, \delta_1, \ldots \quad \gamma_2, \delta_2, \ldots$$

le radici dei polinomi $f_1(x), f_2(x), \ldots$ Non può essere indefinitamente

$$\lfloor \gamma_h \rfloor = \lfloor \delta_h \rfloor$$

perché il polinomio $f_0(x)$ ha radici distinte. Dopo un numero finito di passaggi ricadiamo nel caso delle radici con diversa parte intera. Concludiamo quindi con il

Teorema 2. – Ogni frazione continua che sia periodica dopo un numero finito di quozienti parziali converge ad un irrazionale quadratico. Viceversa ogni irrazionale quadratico ha uno sviluppo in frazione continua periodico da un certo posto in poi.

2.4.2 Il teorema di Galois

Galois ha dimostrato il teorema sulle frazioni continue immediatamente periodiche quando era ancora allievo al Collegio Louis-Le-Grand. Si tratta di un risultato notevole, indipendentemente dalle considerazioni sulla giovane età dell'autore.[15]

Teorema 3. – Se un'equazione ha una radice puramente periodica γ, l'equazione ha un'altra radice δ il cui valore si ottiene dividendo -1 per la frazione puramente periodica il cui periodo è l'inverso di quello di γ.

Dimostrazione. Galois si limita a considerare[16]

$$x = [\overline{a, b, c, d}\,].$$

$$X = a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \cfrac{1}{X}}}} \tag{2.11}$$

[15]Si veda (Galois 1976, pp. 364-377). Un'esposizione del risultato di Galois si trova anche in (De Nuccio 2001).

[16]Si veda la nota 11.

L'equazione (2.11) può essere riscritta:

$$\frac{1}{a-X} = -\left(b + \cfrac{1}{c + \cfrac{1}{d + \cfrac{1}{X}}} \right). \tag{2.12}$$

Procedendo...

$$-X = \cfrac{1}{d + \cfrac{1}{c + \cfrac{1}{b + \cfrac{1}{a-X}}}} \tag{2.13}$$

Dunque

$$\frac{-1}{[\overline{d, c, b, a}]}$$

è l'altra radice dell'equazione. $\square$

Esempio 8. – l'equazione

$$x^2 - 10x - 6 = 0$$

ha le radici

$$5 \pm \sqrt{31}.$$

Abbiamo

$$5 + \sqrt{31} = [\overline{10, 1, 1, 3, 5, 3, 1, 1}],$$
$$\frac{-1}{5 - \sqrt{31}} = [\overline{1, 1, 3, 5, 3, 1, 1, 10}]. \quad \square$$

Osservazione 4. – Una frazione continua puramente periodica

$$\gamma = [\overline{c_0, c_1, \ldots, c_n}]$$

è tale che $c_0 \geq 1$. Anche $c_n \geq 1$ e dunque

$$\gamma > 1, \quad -1 < \frac{-1}{\gamma} < 0.$$

Vediamo ora il risultato reciproco.

TEOREMA 4. – Siano γ, δ le due radici reali di un'equazione di secondo grado e sia

$$\gamma > 1, \quad -1 < \delta < 0.$$

Allora lo sviluppo in frazione continua di γ è puramente periodico.

Dimostrazione. Per il Teorema di Lagrange, lo sviluppo di γ deve essere periodico da un certo posto in poi. Si tratta di dimostrare che è *immediatamente* periodico. Sia dapprima l'antiperiodo di lunghezza 1.

$$\gamma = [p, \overline{a, b, c, d}] = p + \frac{1}{A}.$$

Con

$$x \leftarrow p + \frac{1}{x},$$

la prima trasformata ha la radice A.

Allora ha anche la radice $\frac{-1}{B}$, dove $B = [d, c, b, a]$. L'equazione originale ha la radice

$$p + \frac{1}{-\frac{1}{B}} = p - B.$$

$p - B$ è compreso tra 0 e -1 se e solo se $\lfloor B \rfloor = p$, ossia $d = p$, e

$$\gamma = [\overline{d, a, b, c}].$$

La stessa argomentazione si applica a

$$\gamma = [p, q, \overline{a, b, c, d}\,].$$

In questo caso otteniamo

$$-1 < p - \frac{1}{B - q} < 0. \tag{2.14}$$

Ora, osserva Galois, la quantità $p - \frac{1}{B-q}$ verifica la disuguaglianza (2.14) se e solo se

$$\frac{1}{B - q} = p + \theta, \quad \text{con } 0 < \theta < 1,$$

ossia

$$\left\lfloor \frac{1}{B-q} \right\rfloor = p.$$

Poiché $B > q$ e $B - q < 1$, abbiamo

$$\lfloor B \rfloor = q.$$

Dunque

$$B = [q, p, \dots]$$

e

$$\gamma = [\overline{c, d, a, b}].$$

Galois lascia al lettore il completamento dell'argomentazione. È molto facile, però, dare una forma strutturata a ciò che Galois trascura.

Proposizione 1. – Supponiamo che, per ogni n-upla di interi $c_0, c_1, \dots, c_{n-1}$, con $c_i \geq 1$ e per ogni ξ reale, dalla disuguaglianza

$$-1 < c_0 + \cfrac{1}{c_1 + \ddots + \cfrac{1}{c_{n-1} - \xi}} < 0$$

si tragga la conclusione che

$$\xi = [c_{n-1}, \dots, c_1, c_0, \dots].$$

Allora la proprietà si può estendere ad ogni $n+1$-upla.

Dimostrazione. Sia

$$-1 < c_0 + \cfrac{1}{c_1 + \ddots + \cfrac{1}{c_{n-1} + \cfrac{1}{c_n - \xi}}} < 0,$$

e poniamo

$$\eta = -\frac{1}{c_n - \xi}.$$

Abbiamo allora

$$\eta = [c_{n-1}, \dots, c_1, c_0, \dots],$$

e, essendo,

$$\xi = c_n + \frac{1}{\eta},$$

ne deduciamo la proprietà richiesta. $\square$

Osservazione 5. – Sia $a = \lfloor\sqrt{n}\rfloor$, con n non quadrato. Allora il polinomio

$$(x - a - \sqrt{n})(x - a + \sqrt{n}) = x^2 - 2ax + (a^2 - n)$$

ha una radice maggiore di 1 ed una radice in $(-1, 0)$.

Osservazione 6 (Galois). – Supponiamo che un'equazione di secondo grado abbia una radice il cui sviluppo in frazione continua sia non solo periodico ma anche simmetrico. Allora l'equazione ha la forma

$$ax^2 - bx - a = 0. \tag{2.15}$$

In effetti, se γ è una radice, l'altra radice deve essere $-\gamma^{-1}$. Abbiamo allora

$$\gamma x^2 - (\gamma^2 - 1)x - \gamma = 0.$$[17]

Viceversa, se è data un'equazione della forma (2.15) si verifica immediatamente che ha una radice positiva maggiore di 1 ed una fra 0 e -1. $\square$

2.4.3 Lo sviluppo di $\sqrt{n}$

Sia $a = \lfloor\sqrt{n}\rfloor$. L'equazione

$$(x - a)^2 - n$$

ha una radice $\gamma = a + \sqrt{n}$ puramente periodica (si veda l'Osservazione (5)). Quindi

$$a + \sqrt{n} = [\overline{c_0, c_1, \dots, c_{k-1}, c_k}].$$

Allora

$$\sqrt{n} = [c_0 - a, c_1, c_2, \dots, c_{k-1}, c_k, c_0, c_1 \dots, c_{k-1}, c_k, c_0 \dots].$$

D'altra parte

$$\frac{-1}{a - \sqrt{n}} = [\overline{c_k, c_{k-1}, \dots, c_1, c_0}],$$

[17]Si noti che una tale equazione può ridursi a coefficienti interi.

e quindi

$$\sqrt{n} = [a, c_k, c_{k-1}, \dots, c_1, c_0, c_k, c_{k-1}, \dots].$$

Ne segue che

$$c_0 = 2a, c_1 = c_k, c_2 = c_{k-1}, \dots$$

Ad esempio, come abbiamo visto a pag. 23,

$$\sqrt{19} = [4, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, 2, 1, \dots].$$

2.5 Dimostrazione di Ballieu del teorema di Galois

Galois nella sua prima memoria che abbiamo esaminato utilizza il metodo di Lagrange per analizzare un esempio (dato dall'equazione $3x^2 - 16x - 18 = 0$).[18]

Tuttavia, come abbiamo visto, non utilizza il metodo di Lagrange per dimostrare il suo risultato. Una dimostrazione che utilizza il metodo di Lagrange è data da Ballieu, in (Ballieu 1942). Ecco in breve questa dimostrazione.

Notiamo che data

$$f(x) = ax^2 + bx + c \tag{2.16}$$

i coefficienti di

$$\phi(x) = -x^2 f\left(n + \frac{1}{x}\right) = \alpha x^2 + \beta x + \gamma \tag{2.17}$$

sono dati da

$$\begin{aligned} \alpha &= -(an^2 + bn + c) = -f(n), \\ \beta &= -(b + 2an) = -f'(n), \\ \gamma &= -a = -\frac{f''(n)}{2}. \end{aligned} \tag{2.18}$$

Reciprocamente, abbiamo

$$f(x) = -(x-n)^2 \phi\left(\frac{1}{x-n}\right) \tag{2.19}$$

[18] Cfr. (Galois 1976, p. 375).

e quindi

$$\begin{aligned} a &= -\gamma, \\ b &= -\beta + 2\gamma n, \\ c &= -\gamma n^2 + \beta n - \alpha. \end{aligned} \tag{2.20}$$

Per comodità, introduciamo anche il polinomio

$$F(x) = -\gamma x^2 + \beta x - \alpha. \tag{2.21}$$

Se ora l'equazione di secondo grado (2.16) ha una radice puramente periodica ξ, deve essere $\xi > 1$ e l'altra radice deve essere compresa tra -1 e 0, perché queste condizioni sono realizzate dopo un numero finito di passi (si consideri il comportamento delle radici per le successive trasformazioni di Lagrange esaminato a pag. 2.4.1).

Vediamo che le condizioni sono anche sufficienti. In effetti se un'equazione ha una radice positiva maggiore di uno ed una radice compresa tra -1 e 0, tutte e successive trasformate hanno questa proprietà.

Considerando i valori in -1,0,1, avremo, per un'equazione della forma (2.16), ottenuta con una certa parte intera n,

$$a - b + c > 0, c < 0, a + b + c < 0.$$

Tenendo conto delle (2.20), abbiamo

$$a - b + c = -\gamma(n+1)^2 + \beta(n+1) - \alpha = F(n+1) > 0$$

e

$$c = -\gamma n^2 + \beta n - \alpha = F(n) < 0.$$

Il polinomio $F(x)$ ha una sola radice positiva (si rammenti che γ e α hanno segni discordi) e dunque la parte intera della radice è n. Ne segue che dall'equazione con coefficienti α, β, γ, tramite la radice positiva di $F(x)$ possiamo risalire ai coefficienti a, b, c.

Se dunque un'equazione si ripete accade lo stesso dell'equazione precedente.

Esempio 9. – Consideriamo l'equazione

$$x^2 - 10x - 4 = 0,$$

la quale ha le radici $5 \pm \sqrt{29}$. Abbiamo

$$5 + \sqrt{29} = [\overline{10, 2, 1, 1, 2}\,].$$

Possiamo anche 'procedere a ritroso'. Scriviamo l'equazione corrispondente alla (2.21):

$$4x^2 - 10x - 1 = 0.$$

Poiché si ha un cambiamento di segno in $(2, 3)$, otteniamo per il quoziente parziale che precede 10, il valore 2. Ora utilizziamo la (2.19), ed otteniamo:

$$4x^2 - 6x - 5 = 0.$$

Allora, per retrocedere ulteriormente, dobbiamo considerare

$$5x^2 - 6x - 4 = 0.$$

Si ha un cambiamento di segno fra 1 e 2, ecc.

Capitolo 3

Costruzioni con riga e compasso

3.1 Una premessa algebrica

Sia K un campo (ad esempio il campo razionale $\mathbb{Q}$) e sia θ un elemento di K per il quale *non vi sia* un elemento $\xi \in K$ tale che $\xi^2 = \theta$ (per esempio $2 \in \mathbb{Q}$ e in $\mathbb{Q}$ non abbiamo $\sqrt{2}$).

Vogliamo costruire un nuovo campo E tale che:

- $K \subset E$ (o meglio: E contenga un'immagine isomorfa di K);
- in E vi sia un elemento ξ tale che
$$\xi^2 = \theta;$$
- E sia il campo *minimo* con questa proprietà.[1]

La costruzione di E può essere effettuata con il procedimento seguente (Kronecker): scegliamo un simbolo ξ e consideriamo tutti i polinomi *formali*

$$a + b\xi, \text{ con } a, b \in K$$

di grado minore di 2. Questo insieme forma un gruppo abeliano per l'addizione. Introduciamo ora un nuovo genere di moltiplicazione, che denotiamo con $\star$:

$$(a + b\xi) \star (c + d\xi) = (ac + bd \cdot \theta) + (ad + bc)\xi$$

[1] La condizione di minimalità va interpretata nel senso che ogni altro campo contenente ξ contenga anche E.

È facile verificare che con l'addizione usuale e con questa moltiplicazione E forma un campo. L'unica verifica significativa è quella dell'esistenza dell'inverso. Consideriamo $a + b\xi$, con a, b non entrambi nulli. Allora l'elemento

$$\frac{a - b\xi}{a^2 - b^2\theta}$$

costituisce l'inverso di $a + b\xi$.[2]

Evidentemente

$$\xi \star \xi = (0 + 1\xi)(0 + 1\xi) = (0^2 + 1^2 \cdot \theta) + (0 \cdot 1 + 1 \cdot 0)\xi = \theta + 0\xi.$$

Se a è un elemento di K, può essere *identificato* con il polinomio $a + 0\xi$ di grado 0. Se a, a' sono elementi di K identificati con i polinomi $a + 0 \cdot \xi, a' + 0 \cdot \xi$,utilizzando lo stesso procedimento di identificazione, si ha: $a \star a' = aa'$.

Possiamo dunque identificare K con il sottocampo di E formato dai polinomi di grado 0. Denotando, per semplicità, il prodotto in E nel modo abituale, abbiamo che l'elemento ξ verifica $\xi^2 = \theta$.

Esempio 10. – Consideriamo $\mathbb{Z}_3$. In questo campo nessun elemento ha quadrato 2. Abbiamo i nove polinomi di primo grado

$$0, \xi, 2\xi, 1, 1 + \xi, 1 + 2\xi, 2, 2 + \xi, 2 + 2\xi.$$

che formano un campo con nove elementi. In questo campo $\xi^2 = 2$. La seconda radice dell'equazione $x^2 - 2 = 0$ è data da $2\xi = -\xi$.

Osservazione 7 (Fondamentale). – Il procedimento con il quale dati un campo K ed un elemento θ privo di radice quadrata si aggiunge a K una radice quadrata di θ si inquadra in un contesto più generale.[3]

- La mancanza di radice quadrata equivale al fatto che il polinomio $x^2 - \theta$ è *irriducibile*;

- Il prodotto $\star$ è definito come il *resto* della *divisione* del polinomio $(a + b\xi)(c + d\xi)$ per $\xi^2 - \theta$;

---

[2] Evidentemente l'inverso è ottenuto moltiplicando 'sopra e sotto' $\frac{1}{a+b\xi}$ per $a - b\xi$.

[3] Che è descritto in tutti i principali testi di algebra. Si veda in particolare il testo ammirevole di Michael Artin: cfr. (Artin 1997, p. 596).

- L'esistenza dell'inverso (che garantisce la struttura di campo) è data dal fatto che un polinomio di primo grado $a + b\xi$ è necessariamente primo con il polinomio irriducibile $\xi^2 - \theta$ e dunque esistono due polinomi $f(\xi), g(\xi)$ tali che

$$1 = f(\xi)(a + b\xi) + g(\xi)(\xi^2 - \theta).$$

Il polinomio $f(\xi)$ (che ha grado al più 1) è l'inverso richiesto.

Sia ora $f(x)$ un polinomio *irriducibile* di grado n. L'insieme dei polinomi formati con il simbolo ξ di grado al più $n-1$ può essere strutturato a campo mediante la ordinaria addizione e definendo il prodotto $\star$ di due polinomi $a(\xi), b(\xi)$ come *resto della divisione* di $a(\xi)b(\xi)$ *per* $f(\xi)$. In questo modo costruiamo un campo E dove il polinomio $f(x)$ ha almeno una radice. Si noti che il campo E, pensato come spazio vettoriale su K ha *dimensione* uguale al *grado del polinomio* $f(x)$.

In generale, se E è una estensione di K che, pensata come spazio vettoriale su K ha dimensione n, si usa la notazione

$$[E : K] = n.$$

È assai facile dimostrare che, se sono dati tre campi $K \subset E \subset L$, con $[E : K] = n, [L : E] = m$, si ha

$$[L : K] = mn = [L : E][E : K]. \tag{3.1}$$

Esempio 11. – In $\mathbb{Z}_7$ il polinomio $x^3 - 2$ è privo di radici. Consideriamo l'insieme E dei polinomi di secondo grado

$$a + b\xi + c\xi^2.$$

Il prodotto (tra questi 7^3 elementi) è definito semplicemente ponendo, dopo aver eseguito il prodotto nel modo abituale, $\xi^3 = 2$ e quindi $\xi^4 = 2\xi$. Così

$$(2 + \xi^2)(2 - \xi^2) = 4 - \xi^4 = 4 - 2\xi.$$

Nel nuovo ambiente, il polinomio $x^3 - 2$ si decompone in

$$(x - \xi)(x^2 - \xi x + \xi^2) = (x - \xi)(x - 2\xi)(x - 4\xi),$$

perché $\mathbb{Z}_7$ contiene le radici cubiche dell'unità $1, 2, 4$. In questo caso abbiamo aggiunto tutte le radici.

Osservazione 8. – Se $K \subset \mathbb{C}$, scelto arbitrariamente un elemento $\theta \in K$ privo di radice quadrata, esiste certamente un numero *complesso* ξ tale che $\xi^2 = \theta$ e la costruzione di Kronecker consiste nel considerare i *numeri complessi* della forma $a + b\xi$ con $a, b \in K$ e ξ una delle due radici di θ.

Se $\theta \in K \subset \mathbb{R}$ e $\theta > 0$ si ha $E \subset \mathbb{R}$.

3.2 Elementi di geometria

Sia S un insieme di punti nel piano.[4] $\mathcal{L}_S$ sia l'insieme delle linee rette nel piano per due punti di S. $\mathcal{C}_S$ sia l'insieme delle circonferenze aventi centro in un punto di S e raggio uguale alla distanza di due punti di S.

Definizione 5. – Un punto è *costruibile in un passo* da S se

1. È intersezione di due linee di $\mathcal{L}_S$;
2. È intersezione di una linea di $\mathcal{L}_S$ e di una circonferenza di $\mathcal{C}_S$;
3. È intersezione di due circonferenze di $\mathcal{C}_S$.

Analogamente:

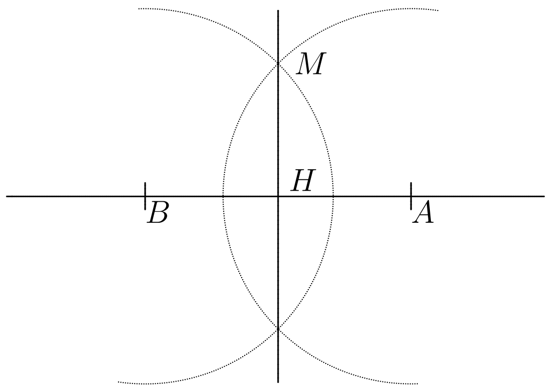
Definizione 6. – Un punto P è *costruibile in n passi* da S quando esiste una successione finita di punti $P_1, P_2, \ldots, P_n$ per la quale

- $P_n = P$;
- Per $i = 1, 2, \ldots, n$ il punto P_i è costruibile in un passo con

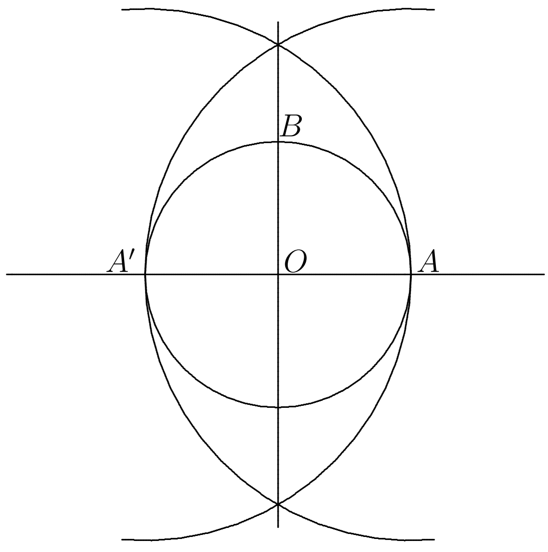
$$S \cup \{P_j : j < i\}.$$

Dati i punti A, B con $A \neq B$ e M possiamo costruire la proiezione di M sulla retta contenente i punti A, B, che denotiamo con (AB). Se $M \in (AB)$ la proiezione è M. Altrimenti si procede come suggerisce la figura:

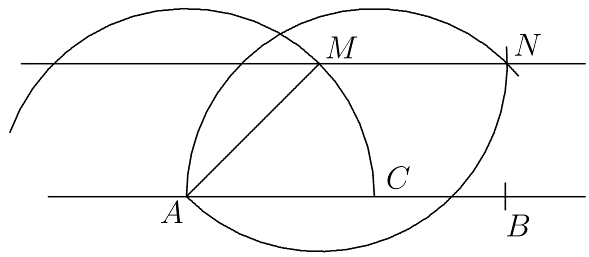
[4] Qui seguo, con qualche modificazione, l'esposizione assai semplice di (Escofier 2001, cap. 5). Si veda anche (Rotman 1998, pp. 129-138). Naturalmente mantiene inalterata la sua eleganza la descrizione di Emil Artin. Si veda (Artin 1944, pp. 80-82) o la più ricca esposizione in (Artin 1988).



La costruzione di una base ortonormale, dati i punti A, O (per ipotesi $\overline{AO} = 1$) è illustrata dalla figura seguente:



Per la costruzione di una linea parallela ad una linea data si può utilizzare la costruzione seguente.



Si tratta della costruzione di un *rombo*.

3.3 Algebra e geometria

Osservazione 9. – S contenga almeno due punti O, A. Si costruisce una base ortonormale formata da O, A, B. Sia $K = \mathbb{Q}(F)$ l'estensione di $\mathbb{Q}$ generata aggiungendo a $\mathbb{Q}$ l'insieme F delle ascisse e delle ordinate dei punti di S. Allora le rette hanno equazioni del tipo

$$ax + by + c = 0, \quad \text{con } a, b, c \in K$$

e le circonferenze hanno equazioni del tipo

$$x^2 + y^2 + ax + by + c = 0, \quad \text{con } a, b, c \in K.$$

Definizione 7. – Diremo che il campo E è una *estensione quadratica* di K se il campo E è ottenibile da K mediante una successione di estensioni

$$K = K_1 \subset K_2 \subset \cdots \subset K_n = E$$

ognuna delle quali si ottiene dalla precedente aggiungendo la radice di un'equazione della forma $x^2 - \alpha_i = 0$.

Se $K \subset \mathbb{R}$ e $\alpha_i \geq 0$ si ha anche evidentemente $E \subset \mathbb{R}$.

Analizziamo le coordinate dei punti costruibili in un passo: P abbia le coordinate (p, q) rispetto alla base. Allora

$$\begin{cases} K(p,q) \text{ coincide con } K, \text{ oppure} \\ K(p,q) \text{ è una estensione quadratica di } K. \end{cases}$$

Abbiamo infatti queste possibilità: le coordinate di P sono date da

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0, \end{cases}$$

oppure da

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0, \end{cases}$$

o infine da

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0. \end{cases}$$

Osservazione 10. – Poiché in un'estensione quadratica E di K

$$[K_i : K_{i-1}] = 2, \text{ oppure } [K_i : K_{i-1}] = 1$$

si ha

$$[E : K] = 2^\nu.$$

Teorema 5. – Il punto $P = (p, q)$ sia costruibile a partire da S, allora:

- Esiste una successione di campi $\{K_i\}_{1 \leq i \leq n}$ tale che

$$K_1 = K, K_n \subset \mathbb{R}$$

  e K_i o coincide con il campo precedente o è una estensione quadratica di questo;

- p e q sono algebrici su K aventi per grado una potenza di 2.

Dimostrazione. Il primo punto della dimostrazione è evidente (si proceda per induzione). Per il secondo punto si osserva che $[K_i : K_{i-1}] = 2$ oppure $[K_i : K_{i-1}] = 1$. □

Abbiamo ora gli elementi necessari per dimostrare l'impossibilità di duplicare un cubo o di trisecare un angolo generico utilizzando solamente la riga ed il compasso. Si tratta di dimostrare che la soluzione di questi problemi dipende da un'equazione irriducibile il cui grado *non è* una potenza di due.

Esempio 12 (Duplicazione del cubo). – Il polinomio $x^3 - 2$ è *irriducibile* in $Q[x]$, perché se fosse riducibile dovrebbe avere una radice razionale. Allora $\sqrt[3]{2}$ è di grado 3 e quindi è impossibile duplicare il cubo con riga e compasso.

Esempio 13 (trisezione dello'angolo). – La costruzione di un angolo θ che sia la terza parte di un angolo dato equivale a

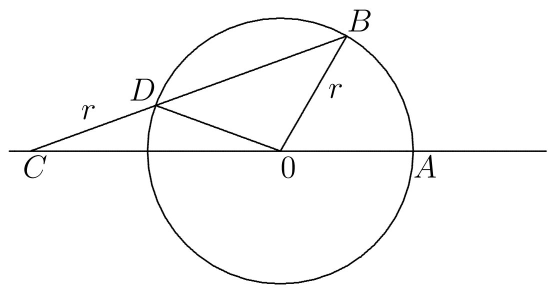
$$4x^3 - 3x - \cos 3\theta = 0.$$

Per $\theta = \frac{\pi}{9}$, si ha

$$8x^3 - 6x - 1 = 0.$$

Il polinomio $8x^3 - 6x - 1$ non ha radici razionali, e quindi è irriducibile. In generale, è impossibile trisecare un angolo con riga e compasso.

Si noti che è molto facile risolvere 'praticamente' i problemi precedenti. Ad esempio, la trisezione dell'angolo è realizzata da Archimede con un semplice procedimento di *inserzione*[5] illustrato dalla figura seguente: si tratta di condurre dal vertice B una semiretta che intersechi la circonferenza in D e la retta OA in C in modo che il segmento CD sia uguale al raggio r. Evidentemente allora $\widehat{DCO} = \frac{1}{3}\widehat{BOA}$.



[5]Si veda (Archimede 1974, p. 327). Una breve discussione sull'uso dei procedimenti di inserzione si trova in (Galuzzi 2002).

3.4 Poligoni regolari

Sia p un numero primo. La determinazione del poligono regolare di p lati dipende dall'equazione $x^p - 1 = 0$. Tolta la radice $x = 1$, si tratta di trovare le altre radici, della forma $\zeta = \cos\theta + i\sin\theta$, del polinomio irriducibile:[6]

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = 0. \tag{3.2}$$

Se il poligono di p lati è costruibile con riga e compasso, allora $\cos\theta$ e $\sin\theta$ sono costruibili e quindi devono appartenere ad un'estensione reale E di $\mathbb{Q}$ di grado 2^n. L'estensione $E(i)$ ha grado 2 su E e quindi

$$[E(i) : \mathbb{Q}] = 2^{n+1}.$$

Poiché $\zeta = \cos\theta + i\sin\theta$ è radice del polinomio irriducibile (3.2) ne segue che $p - 1$ deve essere una potenza di 2.[7]

Si ha dunque che, se il poligono regolare avente il numero primo p di lati è costruibile con riga e compasso, deve essere $p = 2^r + 1$.[8] È dunque impossibile costruire con riga e compasso il poligono regolare di 7 lati.

A Gauss si deve il risultato reciproco: se p è un primo della forma $2^r + 1$, allora il poligono di p lati è costruibile con riga e compasso. Più in generale, ecco il suo risultato:

Teorema 6. – Esiste una costruzione con riga e compasso del poligono regolare di n lati se e solo se

$$n = 2^i p1 p_2 \cdots p_j$$

con $n \geq 3, i \geq 0, \geq 0$ e dove i p_k sono primi di Fermat distinti.[9]

---

[6]Cfr. (Artin 1997, p. 479) per la classica dimostrazione dell'irriducibilità.

[7]Si ha evidentemente $\mathbb{Q} \subset Q(\zeta) \subset E(i)$. Si rammenti la (3.1).

[8]Si noti che, se p è un primo della forma $2^r + 1$ deve essere a sua volta $r = 2^t$.

[9]Ossia primi della forma $2^{2^m} + 1$. Si veda (Křížek, Luca, and Somer 2001, cap. 16).

Capitolo 4

Sull'origine del calcolo differenziale

La linea espositiva che si utilizza oggi per esporre il calcolo differenziale consiste (schematicamente) dei punti seguenti:

- concetto di funzione;
- nozione di limite, continuità;
- rapporto incrementale, limite del rapporto incrementale;
- derivata, proprietà della derivazione, applicazioni;

Tra le applicazioni, una delle più importanti è data certamente dal calcolo della tangente ad una curva.

La definizione di limite si struttura, in genere, nel modo seguente:

Definizione 8. – La funzione $f(x)$ ha per limite l per x tendente a x_0, e si scrive $f(x) \to l$ per $x \to x_0$, quando

$$\forall \varepsilon > 0,\ \exists \delta = \delta(\varepsilon) : 0 < |x - x_0| < \delta \Rightarrow |f(x) - l| < \varepsilon.$$

(Cauchy–Weierstrass)

Conseguentemente si definisce poi la derivata:

Definizione 9. – La derivata di $f(x)$, $f'(x)$, è data da:

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}.$$

Si considera il grafico di $y = f(x)$: nel punto $(x_0, f(x_0))$ la tangente è la retta di equazione
$$y - f(x_0) = f'(x_0)(x - x_0).$$

Il percorso *storico* è assai diverso: nell'antichità si sapeva calcolare (tracciare) la tangente per alcune curve: coniche, spirale, ecc.

Con Descartes e Fermat si arriva alla definizione di curva algebrica di equazione $f(x, y) = 0$: si pone il problema della tangente in un punto ad una curva algebrica.

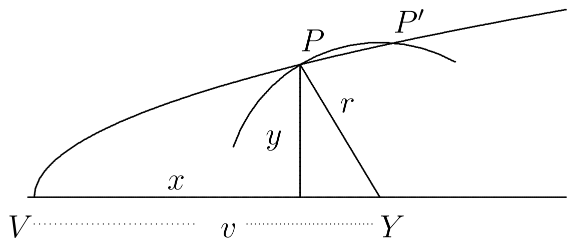
Newton (e Leibniz) riflettendo sul metodo di Descartes forniscono soluzioni progressivamente più generali. (Teorema fondamentale del calcolo... (??))

Il concetto di funzione raggiunge la sua centralità in Eulero, a metà Settecento.

Infine si ha la subordinazione del calcolo alla definizione di limite, con Cauchy. Si giunge così ad una definizione indipendente di integrale definito ed al Teorema fondamentale del calcolo.

La fase ultima del 'rigore' porta alla definizione dei numeri reali (Dedekind, Weierstrass, ecc.).

4.1 Il metodo per le tangenti di Descartes.



$P \in f(x, y) = 0, VY = v$. La circonferenza di centro Y e raggio $PY = r$ intersecherà la curva in P ed in un punto 'vicino' P'. L'equazione della circonferenza è
$$(v - x)^2 + y^2 = r^2.$$

Eliminando y tra le due equazioni
$$f(x, y) = 0, \quad (v - x)^2 + y^2 = r^2,$$

otteniamo una equazione
$$\phi(x,[v,r])=0$$
che deve avere una *radice doppia*.

Esempio chiarificatore[1] di
$$y^2=2px$$
Allora
$$(v-x)^2+2px-r^2=0,$$
ossia
$$x^2+2(p-v)x+v^2-r^2=0.$$
L'equazione deve essere della *forma*
$$x^2-2\alpha x+\alpha^2=0.$$
Dal confronto, si ha
$$v=p+\alpha.$$
Se indichiamo ancora con x l'ascissa del punto generico, abbiamo
$$v=p+x.$$
Abbiamo un metodo, in linea di principio applicabile ad ogni curva algebrica. Ma quali difficoltà dobbiamo affrontare?

Consideriamo un caso molto semplice:
$$f(x,y)=x^3+y^3-1=0,$$
e aggiungiamo l'equazione della circonferenza:
$$(v-x)^2+y^2=r^2.$$
Cosa si ottiene eliminando y?
$$\begin{aligned}&x^6-3\,vx^5+\left(15/2\,v^2-3/2\,r^2\right)x^4+\\&\left(-1+6\,vr^2-10\,v^3\right)x^3+\\&\left(-9\,v^2r^2+15/2\,v^4+3/2\,r^4\right)x^2+\\&\left(-3\,v^5+6\,v^3r^2-3\,vr^4\right)x\\&-1/2\,r^6+1/2+1/2\,v^6+\\&3/2\,v^2r^4-3/2\,v^4r^2=0.\end{aligned}$$

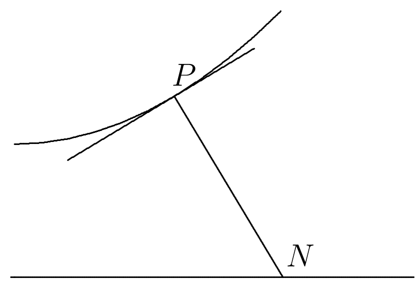
[1] Che non si trova in Descartes.

E dobbiamo confrontare questa equazione con

$$(x-\alpha)^2(x^4+ax^3+bx^2+cx+d).$$

Abbiamo un **metodo** che pare ostacolato da difficoltà insormontabili.

Un'idea fondamentale di Fermat: il problema della tangente è un problema di massimo/minimo. Il segmento condotto da N deve avere lunghezza *minima*.

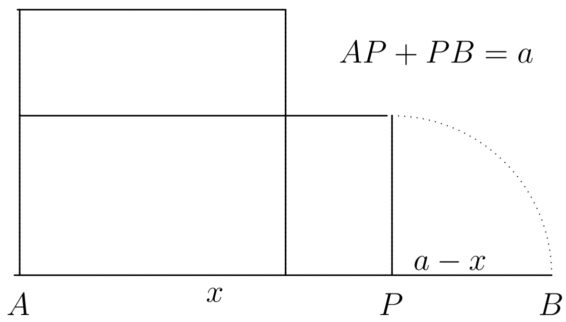


In

$$f(x,y)=0, \quad (v-x)^2+y^2=r^2$$

la quantità r (o r^2) deve essere resa minima.

Come si risolve un problema di minimo o di massimo? L'esempio di Fermat.



Il prodotto $AP \times PB$ deve essere **massimo** con

$$AP+PB=a.$$

Sia $AP = x$: la quantità $x(a-x)$ deve essere massima. Idea (!):

$$x(a-x) = (x+e)(a-x-e)$$

Allora

$$x(a-x) = x(a-x) + e(a-x) - ex - \boxed{e^2}$$

$$0 = 0 + \boxed{e}(a-x-x) - \boxed{0}$$

$$a - 2x = 0 \Rightarrow x = \frac{a}{2}.$$

Un esempio più complesso:

$$f(x,y) = x^4 + y^2 = 1, \quad (v-x)^2 + y^2 = r^2.$$

Sostituendo:

$$r^2 = (v-x)^2 + 1 - x^4.$$

Ponendo ora $x = x + e$ e calcolando la differenza

$$r^2(x+e) - r^2(x),$$

si ha:

$$-e^4 - 4\,xe^3 + \left(1 - 6\,x^2\right) e^2 + \left(-2\,v + 2\,x - 4\,x^3\right) e$$

Allora

$$v = x - 2x^3.$$

van Schooten: trascuriamo ciò che è a coefficiente di $e^2, e^3, \ldots$. Ad esempio, da

$$y = f(x), \quad (v-x)^2 + y^2 = r^2$$

otteniamo

$$(v-x)^2 + f(x)^2 = (v-x-e)^2 + f(x+e)^2.$$

Allora, il calcolo si riduce a

$$2(v-x)\boxed{e} = f(x+e)^2 - f(x)^2.$$

A posteriori:

$$\begin{aligned} 2(v-x)\boxed{e} &= (f(x) + ef'(x))^2 - f(x)^2 \\ &= 2f(x)f'(x)\boxed{e}. \end{aligned}$$

Allora

$$v - x = f(x)f'(x).$$

Attenzione: un'equazione della forma

$$y - f(x) = 0$$

non è un dato molto *naturale* nel contesto delle curve geometriche.

Una struttura che occorre portare alla luce: sia

$$f(x) = \frac{x+1}{x-1},$$

allora

$$v = x + f(x)f'(x) = \frac{x^4 - 3\,x^3 + 3\,x^2 - 3\,x - 2}{(x-1)^3}.$$

Quando si ha il risultato finale, non è facile capire cosa si è fatto. Questo vero soprattutto se si parte da $f(x,y) = 0$.

A posteriori:

$$\phi(x,y) = (v-x)^2 + y^2$$

è una quantità da rendere minima con il vincolo

$$f(x,y) = 0.$$

Allora

$$\nabla f = \lambda \nabla \phi,$$

ossia

$$\begin{pmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial y} \end{pmatrix} = \lambda \begin{pmatrix} \frac{\partial \phi}{\partial x} \\ \frac{\partial \phi}{\partial y} \end{pmatrix} = \begin{pmatrix} -2(v-x) \\ 2y \end{pmatrix}$$

Abbiamo allora

$$v = x - y\frac{\frac{\partial f}{\partial x}}{\frac{\partial f}{\partial y}}.$$

Ancora una volta si tratta di scoprire una struttura. Un esempio ancora:

$$f(x,y) = x^3 + y^3 - 1 = 0.$$

Otteniamo

$$v = \frac{xy^2 - x^2}{y^2}.$$

Si tratta di individuare il ruolo fondamentale dell'operazione

$$f \rightsquigarrow \frac{\partial f}{\partial x}.$$

4.2 Un cenno a Newton

Le conoscenze che Newton possiede quando inizia le sue ricerche:

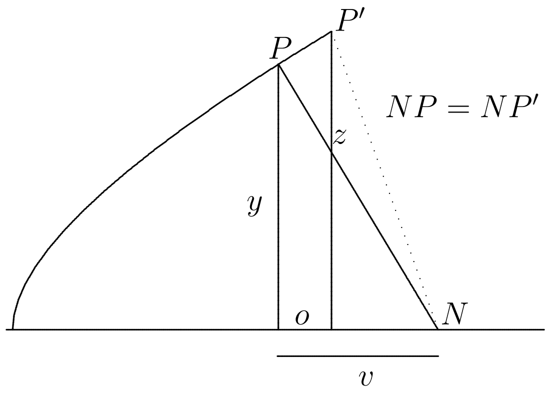
- Il metodo per le tangenti di Descartes con gli arricchimenti di van Schooten;
- (In termini moderni)

$$\int_0^a x^n dx = \frac{a^{n+1}}{n+1};$$

- La linearità di $\int$.

Dopo vari tentativi, Newton considera la curva di equazione

$$ax = y^2 - x^2.$$



Ma ora v è direttamente la *sottonormale*. Accanto all'incremento o (il cambiamento di nome è il suo maggior contributo fondazionale in questo periodo...) introduce l'ordinata z. Considera le due equazioni:

$$a(x+o) = z^2 - (x+o)^2,$$
$$v^2 + y^2 = (v-o)^2 + z^2$$

La seconda può (sempre) essere sostituita da

$$z^2 = y^2 + 2vo.$$

Sostituendo nella prima:

$$ax + ao = y^2 + 2vo - x^2 - 2xo + o^2.$$

Quindi

$$v = \frac{a}{2} + x.$$

Ma ora si ha un approccio più sistematico

$$z^2 = y^2 + 2vo,$$

ma anche, all'occorrenza,

$$z = \sqrt{y^2 + 2vo} = y\left(1 + \frac{vo}{y^2}\right).$$

Ora in generale (ma Newton procede per esempi)

$$f\left(x + o, y + \frac{vo}{y}\right) = 0$$

e quindi

$$\frac{\partial f}{\partial x}\boxed{o} + \frac{\partial f}{\partial y}\,\frac{v}{y}\boxed{o} = 0.$$

Si ritrova il risultato visto. Ma che succede ora sulla 'cellula fondamentale'

$$x^m y^n?$$

Newton non tarda a capire che l'essenza del calcolo è data da

$$x^n \rightsquigarrow n x^{n-1}.$$

Immediatamente gli appare anche il legame con il calcolo inverso

$$x^n \rightsquigarrow \frac{x^{n+1}}{n+1}.$$

Il calcolo differenziale è formato nelle sue linee essenziali.

Capitolo 5

Sulla geometria non euclidea

5.1 Premessa sulla storia della geometria non euclidea

Ancor più della geometria analitica, la geometria non euclidea richiede un'estrema attenzione per evitare di creare una storia artificiale.[1] Una visione molto semplificata (quasi caricaturale) delle vicende della geometria non euclidea può essere così formulata:

a) Negli *Elementi* di Euclide è già presente una 'tensione' non euclidea;

b) L'ininterrotto succedersi dei tentativi di dimostrare il V postulato culmina con Saccheri;

c) Il coraggio intellettuale di Lobatchevsky e Bolyai, infine, conduce al concepimento della geometria non euclidea;

d) L'importanza del legame tra matematica e filosofia è reso evidente da questa vicenda. Con numerose varianti: l'esistenza della geometria non euclidea sarebbe una chiara smentita della filosofia kantiana. Riemann è il più profondo filosofo della geometria, ecc.

Questa brutale schematizzazione non è presente in alcun testo che io abbia in mente: è solo un modello 'negativo' estremo che presento per sviluppare la discussione che segue.

[1] Le considerazioni seguenti sulla geometria non euclidea sono già state presentate in un corso di aggiornamento tenuto a Lecco. Ho introdotto alcune modifiche.

a) Un'affermazione del tipo:

> Già negli Elementi è presente una 'tensione' non euclidea perché Euclide ritarda l'uso del V postulato fino alla proposizione 29...

è molto comune. Ma nell'antichità il problema del V postulato è circoscrivibile ad un desiderio d'avere una buona assiomatica scegliendo una formulazione opportuna (o eliminando un assioma meno 'evidente').

Il ruolo ed il significato della matematica cambiano radicalmente con la 'rivoluzione scientifica'. Nell'antichità la matematica, quando è applicata al mondo fisico, è uno *strumento descrittivo*, estremamente utile, ma che non coglie la *realtà* dei fenomeni.[2]

Con la rivoluzione scientifica il mondo matematico (i punti/enti ideali che si muovono in uno spazio geometrico astratto) sono il *fondamento* per spiegare il comportamento *reale* degli oggetti concreti.[3]

Un brano notissimo del *Dialogo dei Massimi Sistemi*[4] di Galileo:

> Si come a voler che i calcoli tornino sopra gli zuccheri, le sete e le lane, bisogna che il computista faccia le sue tare di casse, invoglie ed altre bagaglie, così quando il filosofo geometra vuol riconoscere in concreto gli effetti dimostrati in astratto, bisogna che difalchi gli impedimenti della materia; che se ciò saprà fare, io vi assicuro che le cose si riscontreranno non meno aggiustatamente che i computi aritmetici.[5]

Perché la matematica (la geometria) è il substrato indispensabile per comprendere il mondo reale, degli oggetti concreti? Questo è un problema nuovo improponibile nel contesto della scienza antica.

Ecco una affermazione di Morris Kline che mi sembra debba essere considerata con estrema attenzione critica.

> L'interesse per questo assioma [l'assioma delle parallele] deriva dal fatto che esso, in quanto assioma, avrebbe dovuto essere una verità evidente. Poiché gli assiomi della geometria sono le proprietà fondamentale dello spazio fisico e vaste branche della matematica

[2]Un insieme di fotografie può essere uno strumento utile (indispensabile) per descrivere la natura di un luogo. Ma non si va al di là della descrizione.

[3]Riferimento d'obbligo sono (Koyré 1972), (Koyré 1976).

[4]Il testo del Dialogo è disponibile al sito: http://www.liberliber.it/biblioteca/g/galilei/

[5](Galilei 1970, p. 252).

> e della fisica usano le proprietà della geometria euclidea, i matematici volevano essere sicuri di basarsi su delle verità. In altre parole, il problema dell'assioma delle parallele non era soltanto un genuino problema fisico, ma il più fondamentale dei problemi fisici possibili.[6]

È con Galileo, Descartes, Newton,... Kant... che si pone il problema della natura della matematica e delle sue verità con speciale riferimento alla sua capacità esplicativa nei confronti del mondo naturale.

Un'affermazione celebre di Kant:

> Io affermo però che in ogni dottrina particolare della natura si può trovare tanta scienza *propriamente detta*, quanta è la *matematica* che si trova in essa.[7]

b) Certamente l'opera di Saccheri ha avuto grande importanza nella vicenda della geometria non euclidea ma la natura della sua ricerca e la (eventuale) influenza della sua opera sono spesso sbrigativamente risolti con la categoria di *precursore* della geometria non euclidea, che sembra essere contraddetta già nel titolo della sua opera: *Euclides ab omni naevo vindicatus*

c) Il coraggio di Lobatchevsky e Bolyai di proporre una geometria contrapposta a quella di Euclide è stato molto grande, ma non bisogna dimenticare che solo con Beltrami e Klein si ha una dimostrazione della *coerenza* della geometria non euclidea.

Si consideri il seguente esempio (piuttosto banale): esistono certamente campi finiti (ad esempio $\mathbb{Z}_p$). Non c'è impedimento logico a priori nel pensare ad una struttura di *corpo finito*: possiamo pensare che per qualche copia di elementi sia

$$ab \neq ba.$$

In questo contesto possiamo dedurre numerosi teoremi... Ma il teorema di Wedderburn (1905) giunge a dirci che ogni corpo finito è in realtà un campo. Siamo dunque in una situazione contradditoria.

---

[6](Kline 1991, p. 1027).

[7](Kant 1959, p. 11). Entrambe le citazioni di Galileo e di Kant si trovano nel bel saggio (Panza 2002) la cui lettura mi ha suggerito di riproporle in questo contesto, ove mi sembra stiano, opportunamente, a dimostrare la stretta connessione della questione della geometria non euclidea con altre importanti problematiche filosofiche.

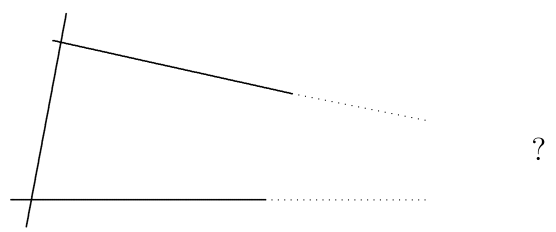
Prima dei modelli di geometria non euclidea *nessuno* poteva garantire la coerenza di essa.[8] Si poteva benissimo immaginare una situazione come quella descritta, il che rende evidente che un certo scetticismo nei confronti della geometria non euclidea non implicava necessariamente ristrettezza di idee.

d) Per una visione adeguata di questo problema non vi è di meglio che consultare i numerosi saggi di Imre Toth. In particolare (Toth 1997).[9]

5.2 Euclide

L'enunciazione originale di Euclide:

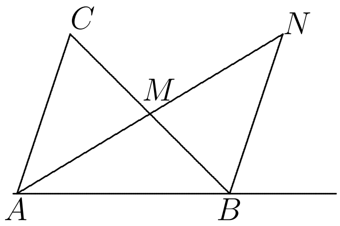
> Se due rette formano con una trasversale, dalla stessa parte, angoli la cui somma è minore di due retti, le rette prolungate finiranno per incontrarsi da quella parte.



Un teorema non-euclideo presente negli Elementi? La proposizione $I.16$: l'angolo esterno è maggiore di ciascuno degli angoli interni non adiacenti.

[8] Si veda anche (Mangione and Bozzi 1993).

[9] Ma si consiglia di consultare la seconda edizione più corretta. A Toth si devono anche numerosi altri contributi fondamentali sulla geometria non euclidea.



$$\widehat{MBN} = \widehat{BCA} \Rightarrow \widehat{BCA} + \widehat{ABC} < \pi$$

Se due rette tagliate da una trasversale si incontrano (ossia si forma un triangolo) la somma degli angoli che formano con la trasversale è minore di due retti.

5.2.1 Una dimostrazione di Hilbert

Hilbert ridimostra la I.16 (Teorema 22, a partire dalla terza edizione (almeno. . .)).[10] In seguito dimostra molte importanti conseguenze: ad esempio:

- Un triangolo con due angoli uguali è isoscele;
- Ogni segmento può essere bisecato.

A prima vista non è facile capire la connessione con la geometria non euclidea del testo di Hilbert. È chiaro solo per chi abbia conoscenza di Legendre, Pasch, ecc.

5.2.2 Osservazioni

- Nella matematica classica le proposizioni sono in genere della forma $\Leftrightarrow$;
- Il postulato fa riferimento al comportamento all'infinito;
- Ha un riscontro empirico assai minore degli altri postulati.

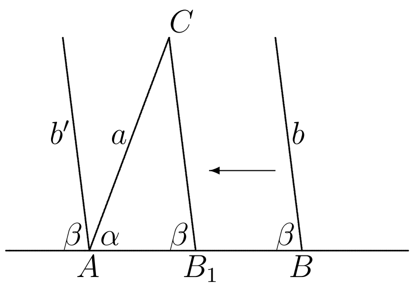
[10] Cfr. (Hilbert 1997, p. 21).

5.3 'Dimostrazioni' del V postulato

Mi limito ad un solo esempio, che mostra il tipo di argomentazioni con le quali si cercava di dimostrare l'assioma delle parallele. In realtà si tratta di sostituzioni dell'assioma con proprietà che si giudicano più evidenti.

5.3.1 Wallis

Si assume che per ogni figura esista una figura simile di grandezza arbitraria.[11]



$$b'||b, \quad b' \text{ nell'angolo adiacente ad } \alpha.$$

Si sposta con continuità la retta b: prima della posizione finale incontra a. Si ha un triangolo AB_1C. Si costruisce il triangolo simile su AB...

5.3.2 Enunciati equivalenti

Cfr. (Bonola 1975, pp. 100-112). Sono equivalenti al V postulato (se si assumono gli assiomi di congruenza e il postulato di Archimede:

- Due rette parallele sono equidistanti;
- Due rette parallele ad una terza sono parallele tra loro.

Se si prescinde dal postulato di Archimede *non è equivalente*:

- La somma degli angoli di un triangolo equivale a due retti.[12]

[11] (Bonola 1975, p.15).
[12] Cfr. (Dehn 1900).

5.4 Saccheri

Dopo la 'riscoperta' da parte di Beltrami, le congetture di Corrado Segre e lo studio di Vailati[13] il percorso intellettuale di Saccheri sembra essere questo: Saccheri ritiene che l'assioma delle parallele, elemento cardine del sistema euclideo, debba avere una dimostrazione di 'pari dignità'. La dimostrazione deve essere come la *consequentia mirabilis*: scaturire dalla sua propria negazione. L'esempio paradigmatico è (oltre al *De Veritate* di Tommaso) la $IX.12$ degli *Elementi*.

Se p primo divide a^n allora p divide a. Supponiamo che p non divida a. Da

$$p\,|a^n = aa^{n-1}$$

segue che p divide a^{n-1}. Alla fine da

$$p\,|a^2 \wedge p \nmid a \Rightarrow p|a.$$

Quindi dall'ipotesi $p \nmid a$ segue esattamente la negazione: $p\,|a$. Questo è lo schema dimostrativo.

Saccheri sa dunque che cosa cercare: non deve cercare una qualsiasi contraddizione: deve dedurre dall'ipotesi dell'esistenza di due rette formanti angoli corrispondenti aventi somma minore di π che non si incontrano (ipotesi assurda) che queste stesse rette si incontrano. La via per giungere a questo risultato non potrà essere l'evidenza immediata.

Saccheri riesce quindi a dimostrare una serie di importanti teoremi prima di arrendersi di fronte a conseguenze che giudica paradossali. Il suo libro è scritto con l'intento preciso di dimostrare il V postulato, ma non si può negare che egli prova una sorta di godimento estetico nell'esplorare il mondo non euclideo (che pure giudica inesistente).[14]

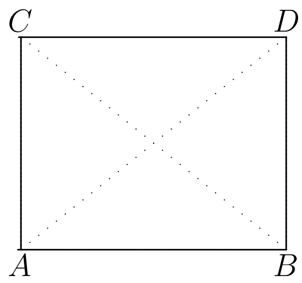
---

[13] Cfr. (Beltrami 1889), (Vailati 1903). Né Beltrami, né Segre e tanto meno Vailati possono essere accusati di un gretto nazionalismo. Tuttavia, nella seconda metà dell'Ottocento ed ancora fino a Novecento inoltrato, il problema di un'identità nazionale della scienza o della cultura è molto sentito. Si pensi a Bertrando Spaventa od a Pierre Duhem.

[14] Tra i molti esempi possibili, si veda dove si vuol procedere im modo 'più elegante': (Saccheri 1986, p. 30).

5.4.1 Un cenno all'*Euclides*

Proposizione I.– Se due segmenti uguali AC, BD formano con il segmento AB angoli uguali dalla stessa parte, anche gli angoli formati con il segmento CD (ossia $\widehat{ACD}$ e $\widehat{BDC}$) sono uguali.

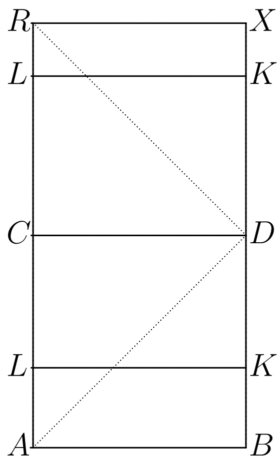


In effetti, tracciati AD, BC dalla I.4 segue che i triangoli ABC e ABD sono uguali. Quindi $AD = BC$. Dalla I.8 segue che i triangoli ACD, BCD sono uguali, quindi anche gli angoli $\widehat{ACD}$ e $\widehat{BDC}$ sono uguali. $\square$

Proposizioni III, IV.– Supponiamo ora che AC, BD siano perpendicolari ad AB (con riferimento alla stessa figura). Allora

- $\widehat{C} = \widehat{D} = \frac{\pi}{2} \Leftrightarrow CD = AB$;
- $\widehat{C} = \widehat{D} > \frac{\pi}{2} \Leftrightarrow CD < AB$;
- $\widehat{C} = \widehat{D} < \frac{\pi}{2} \Leftrightarrow CD > AB$.

Proposizione V.– Se l'ipotesi dell'angolo retto vale anche in un solo caso, essa vale sempre.



Per ipotesi $CD \perp AC \wedge CD \perp BD$. Prolunghiamo i segmenti AC, BD in modo che sia $CR = AC = BD = DX$. Tracciamo AD, DR. I triangolo ACD e RCD sono uguali (per la I.4 degli *Elementi*). Quindi $AD = RD$ e gli angoli $\widehat{ADB}, \widehat{RDX}$ sono uguali. Dall'uguaglianza dei triangoli ABD, RDX si conclude che $RX = AB$. Per quanto dimostrato, sarà $\widehat{R} = \widehat{X}$.

Possiamo ripetere la costruzione con $AR = BR = 2AC = 2BD$ e dunque possiamo supporre che i segmenti $AC = BD$ abbiano lunghezza maggiore di ogni segmento prefissato.

Supponiamo ora di prendere i punti L, K in modo che sia $AL = BK$ e tracciamo LK. Gli angoli $\widehat{ALK}, \widehat{BKL}$ sono uguali. Se non sono retti, possiamo supporre che siano ottusi dalla parte di AB. Allora $LK < AB$. Ma dall'altra parte essi sono acuti, e quindi $LK > RX$. Ne segue $AB > RX$. Ma questo è assurdo. Allora per ogni scelta di $AL = LK$ si ha $LK = AB$. Tutti i quadrilateri birettangoli e isosceli di di base AB sono dunque rettangoli. Se ora partiamo da un rettangolo di base AL possiamo ripetere la costruzione sulla base AL e concludiamo che tuti i quadrilateri birettangoli isosceli sono in realtà rettangoli.

Ci siamo ridotti a dimostrare l'esistenza di un solo rettangolo! Questo rende estremamente plausibile l'idea (in realtà sbagliata, come sappiamo a posteriori) che procedendo con l'analisi si arriverà o ad una conseguenza dei soli primi assiomi od a qualcosa di talmente evidente che sarebbe assurdo negarlo.

Avvertenza. Le due sezioni successive dedicate a Lobatchevsky e Riemann sono, evidentemente, solo suggerimenti per letture personali.

5.5 La geometria non-euclidea: Lobatchevsky

Il modo di procedere ed i risultati di Lobatchevsky: qualche esemplificazione.[15] *Bisogna segnalare l'enorme differenza con Saccheri. Lobatchevsky è profondamente convinto della verità della geometria iperbolica, anche se non possiede alcuno strumento per dimostrare la coerenza. Una presentazione 'euclidea' della geometria non euclidea in (Trudeau 1987). Meglio l'edizione originale, piuttosto della traduzione italiana, per le ragioni che spiego in (Galuzzi 1995).*

5.6 Riemann

Estrema importanza della memoria di Riemann. In traduzione italiana in (Einstein 1967). Cassirer ha dato un'ottima (molto breve) interpretazione di Riemann in (Cassirer 1968). Bisogna però sottolineare il fatto che Riemann scrive prima dei modelli non euclidei. Forse considera la coerenza solo un dettaglio che si può risolvere in breve...

5.7 La coerenza della geometria non euclidea

Presentazione del modello di Beltrami- Klein (o solo di Klein? Un punto storico da chiarire...). Soltanto con i modelli si ha una dimostrazione di coerenza della geometria non euclidea. Bisogna però presentare il modello di Klein senza troppe semplificazioni. Una buona presentazione nella Appendice II di (Lobačevskij 1974). Anche buona la presentazione in (Kline 1991, pp. 1064-1068). Semplificando troppo, dando solo gli aspetti qualitativi si genera scetticismo nei confronti della geometria non euclidea.

Enriques vuole aggiunto un paragrafo: (Enriques 27) al testo di Bonola,

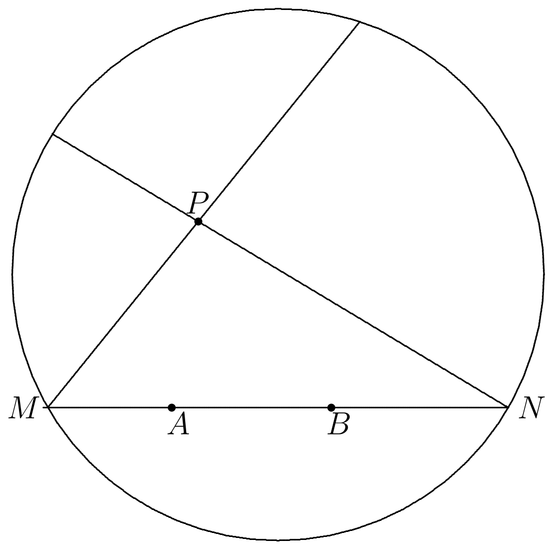
[15](Lobačevskij 1974).

proprio perché senza la presentazione di un modello la questione rimane logicamente in sospeso...[16] Ecco una presentazione schematica.

Conica reale K nel piano (cerchio)

- *Piano*=Regione di punti interni al cerchio
- *Punto*=Punto interno al cerchio
- *Retta*=corda del cerchio
- *Punti consecutivi...*=...
- *Movimento del piano*=Trasformazione proiettiva della regione interna
- *Figure uguali*=Figure trasformabili

Devono ritenersi parallele le corde di K aventi un estremo comune. Per un punto si hanno due parallele.



Il modello non può però avere una sua efficacia se ci si arresta a questo punto. Occorre mostrare (almeno) come si introduce una *distanza* e come si

[16]Si veda anche la parte iniziale di (Mangione and Bozzi 1993).

calcolano gli *angoli* (importanza dei numeri complessi). Se ci si arresta agli aspetti qualitativi si perde ogni efficacia.

$$\mathrm{dist}(AB) = \frac{k}{2} \log{(ABMN)},$$

ove k è un numero negativo (legato alla curvatura di Riemann K da $K = -k^{-2}$).

Poi, volendo che l'angolo retto sia espresso da $\frac{\pi}{2}$, bisogna porre,

$$\mathrm{ang}(ab) = \frac{1}{2i} \log{(abmn)},$$

dove m, n sono le tangenti (immaginarie e coniugate) condotte al cerchio dal vertice dell'angolo formato dalle rette a, b.

$$\mathrm{ang}(ab) = \frac{1}{2i} \log{(abmn)}.$$

L'espressione analitica del birapporto è:

$$\frac{\sin am}{\sin bm} \div \frac{\sin an}{\sin bn}.$$

Rappresentiamo un punto A interno al cerchio in coordinate omogenee, $A = (x_1, x_2, x_3)$; se B è un secondo punto, con $B = (y_1, y_2, y_3)$, poniamo[17]

$$\Omega_{A,B} = x_1y_1 + x_2y_2 - x_3y_3$$

Allora possiamo esprimere la distanza nel modo seguente

$$\mathrm{d}(A, B) = \frac{k}{2} \log \frac{\Omega_{A,B} + \sqrt{\Omega_{A,B}^2 - \Omega_{A,A}\Omega_{B,B}}}{\Omega_{A,B} - \sqrt{\Omega_{A,B}^2 - \Omega_{A,A}\Omega_{B,B}}}.$$

Una formula analoga[18] vale per l'angolo di due rette.

[17] Cfr. (Bonola 1975, p. 150).

[18] Si veda (Bonola 1975, p. 151).

Capitolo 6

Un cenno alle *Grundlagen* di Hilbert

Nel 1899 Hilbert,[1]in un'occasione celebrativa, pubblica un saggio che ha un'importanza fondamentale per i fondamenti della geometria e che diverrà una sorta di manifesto, attraverso le sue numerose edizioni successive, della matematica moderna.[2]

Oltre a proporre un sistema di assiomi rigoroso per la geometria, Hilbert si pone il problema di indagare quali aspetti di essa risultino fondamentali per poter disporre di una 'geometria analitica'. A prima vista il collegamento con la geometria non euclidea sembra problematico. Ma il testo va letto tenendo conto di Riemann. Riemann aveva parlato di *ipotesi* a fondamento della geometria e Hilbert, di conseguenza, propone un sistema di assiomi 'aperto' ai contributi dell'esperienza.[3]

Descartes ha introdotto un *calcolo di segmenti* che corrisponde al calcolo algebrico. Perché questo calcolo funziona? Se consideriamo l'esempio dato da

$$a + ab,$$

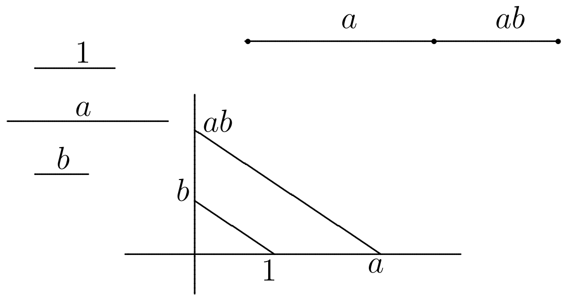
si vede che il calcolo corrisponde (fissato il segmento unitario) alla possibilità

[1]In questa sezione ripropongo gran parte del materiale che ho presentato nelle lezioni finali del corso di Storia della Matematica tenuto per la Silsis, nell'anno accademico 2001-2002 già disponibile in rete all'indirizzo http://www.mat.unimi.it/~galuzzi

[2]Si tratta di (Hilbert 1899). Esiste un'ottima traduzione italiana di Pietro Canetta del testo dell'ultima edizione (anche se 'poco filologica'): (Hilbert 1970). Sulle vicende delle varie edizioni si può vedere (Toepell 1986).

[3](Corry 1997). Meno felice qui Cassirer, che interpreta 'alla Bourbaki'.

di eseguire una serie di costruzioni geometriche che corrispondono alla validità di certi teoremi.



Hilbert analizza con grande attenzione le ragioni che rendono possibile un calcolo come questo.

Un altro oggetto di analisi è il significato dell'*equazione della retta*

$$ax + by + c = 0.$$

Hilbert esamina le ragioni profonde che consentono un calcolo di segmenti tale che l'equazione precedente rappresenti una retta, sia nel caso del prodotto commutativo sia nel caso in cui il prodotto non abbia questa proprietà.

6.1 L'organizzazione del testo

Nel primo capitolo, Hilbert suddivide gli assiomi in cinque gruppi. Si tratta di un'esigenza di maggiore sistematicità rispetto ad Euclide.[4] Ma la suddivisione è anche funzionale allo scoprire cosa può essere ottenuto assumendo, del tutto od in parte, questo o quel gruppo di assiomi.

Il primo gruppo è dato dagli assiomi di collegamento. Si tratta degli *Assiomi piani* I.1 -I.3, e degli *Assiomi spaziali* I.4-I.8. Ecco, ad esempio, il contenuto del primo:

> I.1 Comunque scelti due punti A, B esiste almeno una retta a con $A \in a$ e $B \in a$.[5]

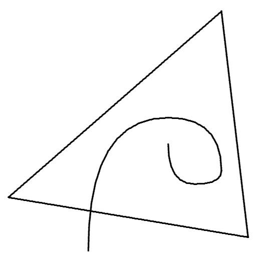
[4]Questo primo capitolo è, ovviamente, necessario. E proprio su di esso innumerevoli autori hanno posta la loro attenzione per eliminare ogni possibile ridondanza ed affinare l'analisi logica. Non va però dimenticato (soprattutto in un eventuale uso didattico) che esso ha un ruolo introduttivo. Ho già espresso questo punto di vista in (Galuzzi 1999b).

[5]Bisogna essere attenti a non interpretare gli assiomi nel senso della appartenenza insiemistica (almeno inizialmente). La retta **non** va pensata come un insieme che contiene

Seguono gli *Assiomi di ordinamento*: II.1-II.4. Particolarmente significativo è l'assioma di Pasch:

> II.4 Assioma di Pasch. Una retta non può 'entrare' in un triangolo senza 'uscirne'. [6]

La figura suggerisce il comportamento che l'assioma vuole proibire: il fatto che una retta possa svolgersi, da un certo punto in poi, all'interno di un triangolo.[7]



Seguono poi gli *Assiomi di congruenza*: III.1-III.5. Tra questi segnalo l'assioma III.4 che corrisponde al trasporto di angoli. e l'assioma III.5:

> III.5 Se per due triangoli ABC e $A'B'C'$ valgono le congruenze
>
> $$AB = A'B', \quad AC = A'C'$$
>
> $$\measuredangle BAC = \measuredangle B'A'C'$$
>
> allora vale anche
>
> $$\measuredangle ABC = \measuredangle A'B'C'$$

(Garantisce l'unicità del trasporto di segmenti...)

Seguono gli assiomi relativi al *parallelismo*, che Hilbert da in due forme

---

i suoi punti. Abbiamo oggetti di tipo *punto*, oggetti di tipo *retta* e un predicato $\in (A, a)$ che può essere vero o falso...Hilberto non utilizza tuttavia né il simbolo di appartenenza $\in$ né il simbolo $\prec$ che io utilizzo in seguito. Ho introdotto questi simboli per comodità.

[6]Naturalmente, nel corso dell'esposizione, Hilbert precisa cosa si deve intendere per triangolo (p. 6), angolo (p. 13), circonferenza (p. 30), ecc.

[7]Gli assiomi precedenti sono già sufficienti per garantire che la retta non possa uscire dal triangolo incidendo sullo stesso lato di ingresso.

IV Siano a una qualsiasi retta e A un punto fuori di a, allora esiste al più una retta che passa per A e non interseca a.

IV* Siano a una qualsiasi retta e A un punto fuori di a, allora esiste una ed una sola retta che passa per A e non interseca a.

(L'assioma si usa nella seconda forma quando *non* si assumono gli assiomi di congruenza)

L'ultimo gruppo di assiomi è quello relativo alla *Continuità*, che Hilbert ancora dà in due forme da utilizzarsi a seconda del contesto:

V.1 Assioma d'Archimede

V.2 Completezza (Nella forma di Dedekind)

6.2 Un esempio di analisi critica

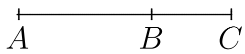
Hilbert dispiega nel testo una notevole sottigliezza critica.

Supponiamo di assumere gli *Assiomi piani* I.1 -I.3, tra i quali

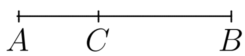
I.1 Comunque scelti due punti A, B esiste almeno una retta a con $A \in a$ e $B \in a$.

Assumiamo anche gli assiomi di *Ordinamento*:

II.1 Se B è posto **fra** A e C allora A, B, C sono punti **distinti** e B è posto anche **fra** C e A.



II.2 Per ogni coppia di punti A, C c'è sempre un punto B, sulla retta AC, tale che C giace fra A e B.



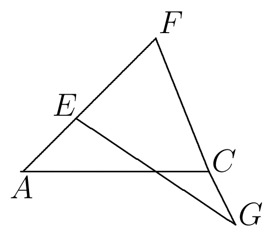
Inoltre:

II.3 Dati tre punti qualsiasi sulla retta ce n'è al massimo uno che giace fra gli altri due.

II.4 Assioma di Pasch.

È possibile dedurre che fra due punti A e C c'è almeno un punto D?

Ecco come è possibile fare la dimostrazione:



Dim. I.3: esiste E che non sta sulla retta AC;

II.2: esiste F in modo che $A \prec E \prec F$;

II.2: esiste G con $F \prec C \prec G$;

Per l'assioma di Pasch, EG interseca AC. $\square$

In modo analogo si può dimostrare: dati tre punti A, B, C ce n'è sempre uno che giace fra gli altri due.

6.3 Hilbert e i teoremi fondamentali della geometria

- Partendo dagli assiomi si può costruire l'intera geometria euclidea e disporre di quel calcolo di segmenti che fonda la geometria analitica.
- Ma è possibile esaminare la struttura, la suddivisione in parti, i collegamenti, ecc. dell'edificio geometrico che si costruisce.
- In questa costruzione emerge il ruolo fondamentale di alcuni teoremi:

Il Teorema di Pascal

Il Teorema di Desargues

Hilbert esamina la geometria dal punto di vista *logico*, ma con l'*esperienza storica*...Non si vuole una qualsiasi ricostruzione con proprietà create ad hoc...

6.4 Calcolo di segmenti con il teorema di Desargues

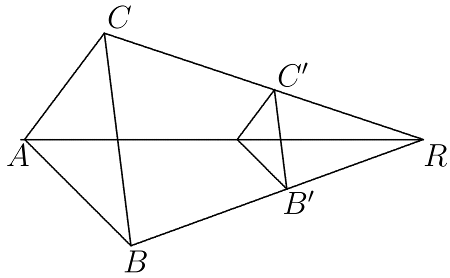
Assumiamo soltanto: [8]

1. Gli assiomi piani tra quelli di collegamento: I.1-I.3;
2. Gli assiomi di ordinamento;
3. IV*.
4. **Non** assumiamo gli assiomi di congruenza, **né** quelli di continuità.

Il teorema di Desargues viene enunciato nella forma più semplice.

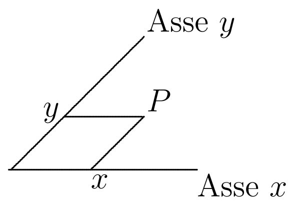
TEOREMA 7. − . Se due triangoli in uno stesso piano hanno i lati corrispondenti paralleli, le rette congiungenti i vertici corrispondenti passano per uno stesso punto o sono parallele.

Se le rette congiungenti i punti corrispondenti passano per uno stesso punto o sono parallele e se due coppie di lati corrispondenti sono paralleli, anche i terzi lati sono paralleli.



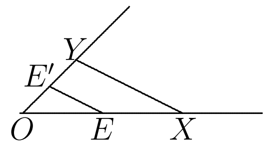
È possibile istituire un *calcolo* di segmenti con soltanto ciò che abbiamo a disposizione?

Non vi sono difficoltà ad introdurre le coordinate, come illustra la figura.



[8]Questo argomento è sviluppato nel cap. V del testo di Hilbert.

Si tratta ora di vedere come, con il materiale a disposizione, si possa arrivare all'equazione della retta. Hilbert fa una osservazione importante: non serve un'analisi del comportamento di *tutti* i segmenti rispetto all'uguaglianza, ma solo di quelli che giacciono sugli assi e con un estremo nell'origine! Per istituire questa uguaglianza *basta il parallelismo*.



Si fissa la retta unitaria EE'. Ora due segmenti (con un estremo in O e giacenti sugli assi) sono uguali in queste condizioni:

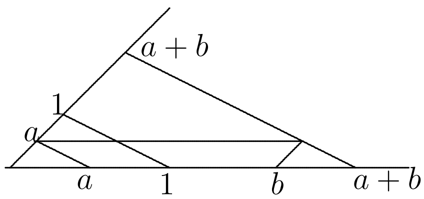
1. se sono entrambi sull'asse x *coincidono*;

2. se sono entrambi sull'asse y *coincidono*;

3. se sono uno sull'asse x e uno sull'asse y, la retta che congiunge i loro estremi diversi da O è *parallela* alla retta unitaria.

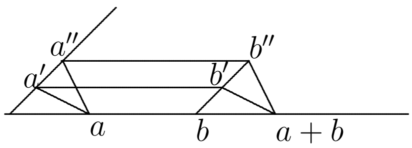
L'uguaglianza dipende dalla scelta della retta unitaria. Ma è possibile istituire una *somma* (su ogni asse) che ne sia indipendente?

Ecco la definizione di *somma*



Si manda da a la parallela alla retta unitaria 11 (per maggiore semplicità ora si utilizzano $a, b, 1$, ecc.: le coordinate) e si trova un segmento 'uguale' ad a. Si manda ora la parallela all'asse x. Da b si manda la parallela all'asse y... Dal punto di intersezione si manda la parallela alla retta unitaria, e si ha $a + b$.

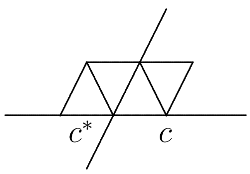
Se si esegue la costruzione in due modi (si osservi che la retta unitaria serve solo a fissare una direzione) otteniamo, se è vero il *teorema di Desargues*, lo stesso risultato (Il teorema va applicato ai triangoli a', a'', a e $b', b'', a + b$).



Con un ragionamento dello stesso tipo si dimostra che

$$a + b = b + a.$$

Evidentemente si ha l'opposto di c, c^* con la costruzione seguente:



Il prodotto di segmenti è definito nel modo abituale, ma ora gli assiomi non bastano a garantire la commutatività.

6.5 Equazione della retta

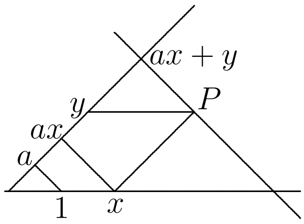
Vogliamo ora vedere come ad una retta si possa associare un'equazione del tipo

$$ax + by + c = 0.$$

Non vi sono difficoltà nel dimostrare che le rette parallele agli assi hanno equazioni del tipo $x = k$ oppure $y = h$. Nel caso generale, poiché per ogni segmento non nullo esiste un inverso rispetto al prodotto (come è facile dimostrare) possiamo ridurci a

$$ax + y + c = 0.$$

Consideriamo la figura.



Se dal punto 1 sull'asse x tracciamo una retta parallela alla retta data otterremo un segmento sull'asse y che indicheremo con a (e che dipende solo dalla posizione della retta data). Se x è l'ascissa di P, ax è il prodotto secondo la definizione vista. Eseguiamo $ax + y$ sommando (relativamente all'asse y. Si ottiene

$$ax + y = c^*,$$

ove c^* è (per la definizione stessa di somma) l'ordinata del punto di intersezione della retta con l'asse y. Sia ora c l'opposto di c^*. Allora

$$ax + y + c = c^* + c = 0.$$

Se ora moltiplichiamo (a sinistra) per un arbitrario segmento b abbiamo l'equazione della retta nella forma solita.[9]

[9]Si noti il 'motore algebrico' dell'analisi. La soluzione delle due equazioni $x = 0$, $a(x - 1) + y = 0$ è evidentemente $(0, a)$. Similmente la soluzione di $ax + y + c = 0$ e $x = 0$ è $(0, -c)$.

Capitolo 7

Computer, storia e didattica

Il computer è entrato nella scuola da molti anni ma soprattutto per rafforzare una didattica di tipo tradizionale (Es. Cabri e la geometria euclidea, Derive e lo studio di funzione).

(Graham, Knuth, and Patashnik 1989) contiene le lezioni tenute a Stanford da Knuth e dai suoi collaboratori (dal 1970) mentre Knuth scriveva *The art of computer programming.*[1] Ecco cosa si trova nell'introduzione: il libro contiene:

> The mathematics he [Knuth] needed for a thorough, well-grounded understanding of computer programs[. . .]

Storia? Il libro [nell'edizione inglese] ha una dedica ad Eulero. . .

7.1 Funzioni generatrici

$$G(z) = g_0 + g_1 z + g_2 z^2 + \cdots = \sum_{n \geq 0} g_n z^n.$$

Possiamo pensare allo sviluppo in serie in almeno due modi (a partire dalla forma chiusa): serie di Taylor, serie formale.

Un vecchio risultato di De Moivre: se $G(z)$ è una funzione razionale, i coefficienti g_k si ottengono con un semplice procedimento ricorsivo.

$$G(z) = \frac{P(z)}{Q(z)}, \quad \partial P < \partial Q.$$

[1] A Knuth si deve la magnnifica creazione del TeX.

Esempio totalmente esplicativo:

$$\frac{\alpha+\beta z}{az^2+bz+c} = g_0 + g_1 z + g_2 z^2 + \dots$$

$$\alpha+\beta z = (az^2+bz+c)(g_0 + g_1 z + g_2 z^2 + \dots)$$

Abbiamo

$$\begin{array}{ccc} \alpha & = & cg_0 \\ \beta & = & bg_0 + cg_1 \\ 0 & = & ag_0 + bg_1 + cg_2 \\ 0 & = & ag_1 + bg_2 + cg_3 \\ \dots & \dots & \dots \end{array}$$

In generale

$$ag_{n-2} + bg_{n-1} + cg_n = 0$$

ossia

$$g_n = -\frac{b}{c}\, g_{n-1} - \frac{a}{c}\, g_{n-2}$$

Dopo che abbiamo calcolato g_0 e g_1 il calcolo dei termini successivi si fa per ricorrenza.

Esempio.

$$\frac{1}{1-x^2} = 1 + 0 \cdot x + ?$$

$$a = -1, b = 0, c = 1, g_0 = 1, g_1 = 0.$$

Allora

$$g_2 = -\frac{0}{1} g_1 - \frac{-1}{1} g_0 = 1,$$

$$g_3 = -\frac{0}{1} 1 - \frac{-1}{1} 0 = 0, \dots$$

$$\frac{1}{1-x^2} = 1 + x^2 + x^4 + \dots$$

(Indipendentemente dal calcolo differenziale)

Reciprocamente: se è data una serie ricorrente, e conosciamo i valori iniziali, possiamo risalire alla funzione razionale che la genera. Supponiamo di avere

$$g_n = 2g_{n-1} - 3g_{n-2}, g_0 = 0, g_1 = 1.$$

Allora
$$-\frac{b}{c} = 2, -\frac{a}{c} = -3.$$
Possiamo porre $a = 3$, allora $c = 1$ e $b = -2$. Poi
$$\alpha = 1g_0 = 0, \beta = -2g_0 + cg_1 = 1.$$
Quindi
$$\frac{2z}{3z^2 - 2z + 1} = 2\,z + 4\,z^2 + 2\,z^3 - 8\,z^4 + \dots$$

7.1.1 Ancora i numeri di Fibonacci

$$f_n = f_{n-1} + f_{n-2}, \quad f_0 = 0, f_1 = 1.$$
Allora:
$$-\frac{b}{c} = 1,\ -\frac{a}{c} = 1.$$
Poniamo $c = -1$, allora $a = b = 1$. Poi
$$\alpha = cf_0 \Rightarrow \alpha = 0,$$
$$\beta = bf_0 + cf_1 \Rightarrow \beta = c = -1$$
Otteniamo la funzione generatrice
$$\frac{z}{1 - z - z^2}.$$

Osservazione 11. – Decomposizione in fratti semplici.
$$\frac{P(z)}{Q(z)} = \frac{P(z)}{(z-\alpha)(z-\beta)(z-\gamma)}$$
Allora
$$\frac{P(z)}{Q(z)} = \frac{A}{z-\alpha} + \frac{B}{z-\beta} + \frac{C}{z-\gamma}$$
Quindi
$$\frac{P(z)}{Q(z)}(z-\alpha) = A + \frac{B(z-\alpha)}{z-\beta} + \frac{C(z-\alpha)}{z-\gamma}$$

Usando la regola di L'Hôpital:

$$A = \frac{P(\alpha)}{Q'(\alpha)}$$

Dalla serie geometrica:

$$\frac{A}{z-\alpha} = -\frac{A}{\alpha}\left(1 + \frac{z}{\alpha} + \frac{z^2}{\alpha^2} + \dots\right)$$

Quindi

$$\frac{P(z)}{Q(z)} = -\left(\frac{A}{\alpha} + \frac{B}{\beta} + \frac{C}{\gamma}\right) - \left(\frac{A}{\alpha^2} + \frac{B}{\beta^2} + \frac{C}{\gamma^2}\right) z + \dots \qquad \square$$

Applichiamolo ai numeri di Fibonacci, ponendo, per semplicità

$$\alpha = \frac{\sqrt{5}-1}{2}.$$

La seconda radice è

$$-(1+\alpha) = -\frac{1}{\alpha}.$$

Si ha

$$\frac{z}{1-z-z^2} = \frac{1}{5}\left[\frac{\alpha-2}{z-\alpha} - \frac{\alpha+3}{z+1+\alpha}\right].$$

Con un po' di pazienza ...

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

7.2 Un problema di Polya

In quanti modi possiamo pagare 10 centesimi con monete da 1,2,5 centesimi? Si tratta di decidere il numero delle soluzioni intere positive di

$$x_1 + 2x_2 + 5x_3 = 10.$$

Possiamo visualizzare i pagamenti fatti con 2 centesimi, ad esempio, come una scelta entro l'allineamento simbolico

$$\boxed{2}^0 + \boxed{2}^1 + \boxed{2}^2 + \boxed{2}^3 + \cdots$$

oppure una scelta in

$$1 + z^2 + z^4 + z^6 + \dots$$

dove l'esponente 0,2,4,6,... sta ad indicare un pagamento privo di monete da 2 centesimi o con una moneta, o con due monete, ecc. Ora, se consideriamo gli allineamenti

$$\begin{aligned} &1 + z + z^2 + z^3 + \dots \\ &1 + z^2 + z^4 + z^6 + \dots \\ &1 + z^5 + z^{10} + z^{15} + \dots \end{aligned}$$

un modo per pagare è dato dalla scelta di un elemento in ogni serie formale, in modo che la somma degli esponenti valga 10. Ad esempio scegliendo

$$z^5, z^4, z.$$

nei tre allineamenti. Ma si tratta esattamente di calcolare il coefficiente del termine z^{10} nel prodotto delle tre serie!

Evidentemente

$$1 + z^k + z^{2k} + z^{3k} + \dots = \frac{1}{1 - z^k}$$

Si tratta allora di calcolare il coefficiente del termine di grado 10 in

$$\frac{1}{1-z} \cdot \frac{1}{1-z^2} \cdot \frac{1}{1-z^5}$$

Otteniamo dallo sviluppo in serie:

$$1 + z + 2z^2 + 2z^3 + 3z^4 + 4z^5 + +5z^6 + 6z^7 + 7z^8 + 8z^9 + 10z^{10} + \dots$$

7.2.1 Ancora Fibonacci

Poniamo ora, per comodità:[2]

$$f_{n+1} = f_n + f_{n-1} \quad (n \geq 1, f_0 = 0, f_1 = 1).$$

Sia $f(x) = \sum_{n \geq 0} f_n x^n$. Allora

$$\sum_{n \geq 1} f_{n+1} x^n = \frac{f(x) - x}{x}$$

[2]Si veda anche la parte iniziale di (Wilf 1994).

Anche

$$\sum_{n\geq 1} f_{n-1}x^n = xf(x).$$

Quindi

$$\frac{f(x)-x}{x} = f(x) + xf(x)$$

Risolvendo

$$f(x) = \frac{x}{1-x-x^2}.$$

Capitolo 8

La ‘matematica moderna’

8.1 Bourbaki

Nel secolo scorso, all’inizio degli anni Sessanta (in Italia, ma non solo in Italia) era molto diffusa l’idea che la matematica avesse subito cambiamenti molto radicali nell’ambito della ricerca. Di modo che fosse possibile (e necessario) contrapporre esplicitamente la ‘matematica moderna’ alla matematica dei tempi precedenti. Di questo cambiamento era giudicato interprete autorevole soprattutto il gruppo di matematici riunito sotto lo pseudonimo di Bourbaki.[1]

Per seguire il corso dei tempi appariva necessario adeguare anche l’insegnamento secondario a ciò che avveniva nell’ambito della ricerca e in quegli anni si sono compiuti numerosi ed importanti tentativi per rinnovare l’insegnamento della matematica nella scuola secondaria ispirandosi, in modo più o meno radicale a Bourbaki.[2]

Oggi il prestigio di Bourbaki come ‘working mathematician’ sembra diminuito e, come spesso accade, molti dei più ferventi sostenitori d’un tempo hanno sviluppato atteggiamenti di rifiuto radicale della matematica bourbakista.

A livello di insegnamento secondario permangono cospicue tracce dell’impostazione bourbakista; ma spesso prive di motivazioni o di quegli sviluppi che ne sarebbero conseguenze naturali. Talvolta, senza la necessaria coscien-

[1] Per qualche prima informazione su Bourbaki si veda (Beaulieu 1994).

[2] Ho sviluppato questo argomento in (Galuzzi 2001) e in (Galuzzi, Neubrand, and Laborde 1998; Galuzzi and Neubrand 1998).

za critica, si giustappongono temi di impostazione anti-bourbakista senza che il contrasto venga avvertito. Tutto ciò, ovviamente, genera confusione.

Alcuni aspetti dell’impostazione bourbakista, ad esempio il rilievo assegnato alle *strutture matematiche* hanno però, a mio giudizio, il carattere di conseguenza *necessaria* dello sviluppo storico. In questo sviluppo,– in particolare nella storia dell’algebra,– si coglie un cambiamento molto radicale che, a partire da Galois e giungendo a conclusione negli anni tra le due guerre del secolo scorso, pone in primo piano certi caratteri strutturali che segnano una diversità profonda con la matematica precedente.

Cercheremo di valutare la portata di questo cambiamento con qualche riflessione legata alla genesi della struttura di gruppo.

8.2 Un cenno alla teoria di Galois

La necessità di ’aggiungere’ soluzioni di equazioni algebriche ad un patrimonio numerico preesistente ha spesso motivazioni geometriche. Se, fissato un segmento unitario $\mathbf{u}$, supponiamo di conoscere tutti i segmenti della forma $\frac{m}{n}\mathbf{u}$, abbiamo visto che (cfr. la Sezione 2.2) questa conoscenza non è sufficiente per costruire una geometria ove la diagonale di un quadrato sia ‘esprimibile’. Ciò significa che dobbiamo ‘aggiungere’ un nuovo segmento, $\sqrt{2}$, soluzione dell’equazione $x^2 - 2 = 0$, ai segmenti precedenti. Ora è naturale che questo nuovo segmento possa essere utilizzato al pari degli altri: possa essere raddoppiato o diviso in parti: che si abbia cioè $2\sqrt{2}$ e $\frac{\sqrt{2}}{n}$. In breve: dobbiamo avere disponibile ogni funzione razionale di $\sqrt{2}$.

In termini più precisi, ciò significa che passiamo dal campo $\mathbb{Q}$ dei numeri razionali a $\mathbb{Q}(\sqrt{2})$: il minimo campo che contiene sia $\mathbb{Q}$ sia $\sqrt{2}$. Poiché $\left(\sqrt{2}\right)^2 = 2$, si vede facilmente che $\mathbb{Q}(\sqrt{2})$ è formato da tutti gli elementi del tipo

$$a + b\sqrt{2}, \tag{8.1}$$

con $a, b \in \mathbb{Q}$.

In effetti in questo esempio vi è qualche forzatura ,che trova riscontro nel fatto che, in realtà, abbiamo aggiunto *entrambe le radici* di $x^2 - 2 = 0$. Non siamo a partiti solo dai segmenti della forma $\frac{m}{n}\mathbf{u}$, ma dai segmenti $\pm\frac{m}{n}\mathbf{u}$: questo perché l’esperienza ha mostrato che è utile disporre anche delle quantità negative. Ma allora la (8.1) consente di ottenere anche $-\sqrt{2}$.

Ancora, un'esperienza secolare ha mostrato l'importanza dei numeri complessi. Possiamo dunque ritenere sufficientemente motivata una situazione come questa: sia $f(x) \in K[x]$ un polinomio (senza radici multiple), ove K è un 'campo' che si ottiene da $\mathbb{Q}$ 'aggiungendo' certe quantità reali o complesse, in numero finito, soluzioni di equazioni algebriche.

Le radici $\alpha, \beta, \gamma, \ldots$ sono allora elementi di $\mathbb{C}$. Ma il passaggio da K a $\mathbb{C}$ è eccessivo. È come se volessimo risolvere contemporaneamente tutti i problemi corrispondenti a tutte le possibili equazioni $F(x) = 0$ con $F(x)$ un arbitrario polinomio a coefficienti reali.

È invece naturale considerare $E = K(\alpha, \beta, \gamma, \ldots)$ il *minimo campo* che contiene $\alpha, \beta, \gamma, \ldots$ Ciò che è indispensabile per risolvere il problema.

Un generico elemento di E ha la forma

$$\gamma = \frac{P(\alpha, \beta, \gamma, \ldots)}{Q(\alpha, \beta, \gamma, \ldots} \tag{8.2}$$

dove $\alpha, \beta, \gamma, \ldots$ corrisponde ad una scelta delle radici di $f(x)$. Se operiamo una scelta differente, è naturale attendersi che l'elemento γ muti il suo valore. Ma se accade che γ sia un elemento di K è invece naturale attendersi che la nostra scelta *non ne muti* il valore: cambiando i nomi dei nuovi 'segmenti' $\alpha, \beta, \gamma, \ldots$ non dobbiamo alterare la natura dei segmenti 'vecchi'.

Possiamo dunque pensare che nell'insieme S di tutte le permutazioni di $\alpha, \beta, \gamma, \ldots$ solo alcune tra esse debbano essere considerate. Tutte e sole quelle che non alterano i valori di quelle funzioni di $\alpha, \beta, \gamma, \ldots$ che assumono un valore nel campo K. Vediamo un esempio.

Esempio 14. – Sia

$$f(x) = (x^2 - 2)(x^2 - 3).$$

Le radici sono

$$\alpha = \sqrt{2}, \beta = -\sqrt{2}, \gamma = \sqrt{3}, \delta = -\sqrt{3}.$$

Un elemento generico di E ha la forma (come si può verificare facilmente)

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$$

con $a, b, c, d \in \mathbb{Q}$. Evidentemente la funzione

$$f(x, y, z, t) = (xy - zt)$$

valutata su $\alpha, \beta, \gamma, \delta$ assume il valore 1, e mantiene lo stesso valore se scambiamo α con $-\alpha$ o β con $-\beta$ o eseguiamo entrambi gli scambi. Ma cambia il suo valore se scambiamo invece α con γ lasciando fisse β e δ.

Se indichiamo le radici con i simboli 1, 2, 3, 4 le permutazioni

$$\begin{array}{c} \mathbf{1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \end{array} \tag{8.3}$$

sono tutte e sole quelle che lasciano invariato il valore della funzione proposta. Si può dimostrare che ogni funzione delle radici che ha valore razionale è invariante per tutte e sole queste permutazioni e che viceversa ogni funzione invariante per queste permutazioni ha valore razionale.

Se si esaminano queste permutazioni, si scopre facilmente che formano un insieme moltiplicativamente chiuso.[3] Precisamente si ha la seguente tavola di composizione:

	$\mathbf{1}$	σ	τ	ρ
$\mathbf{1}$	$\mathbf{1}$	σ	τ	ρ
σ	σ	$\mathbf{1}$	ρ	τ
τ	τ	ρ	$\mathbf{1}$	σ
ρ	ρ	τ	σ	$\mathbf{1}$

Abbiamo dunque un *gruppo* di permutazioni. La situazione ‘geometrica’ che corrisponde a considerare noti anche i segmenti $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ impone dunque che una volta scelti i ‘nomi’, ossia i simboli $1, 2, 3, 4$ per denotare questi segmenti, essi possano essere modificati solo con le permutazioni $\mathbf{1}, \sigma, \tau, \rho = \sigma\tau = \tau\sigma$. Queste sono le ‘simmetrie’ ammissibili. $\square$

Il contributo fondamentale di Galois allo sviluppo dell’algebra può essere schematizzato in questo modo:

[3] Il prodotto è la composizione di funzioni. Ad esempio $\sigma\tau(3) = \sigma(\tau(3)) = \sigma(4) = 4$.

- per ogni polinomio $f(x) \in K[x]$ possiamo calcolare esplicitamente (e senza conoscerne le radici) il gruppo G formato dalle permutazioni delle radici che, applicate alle funzioni di queste che assumono valore in K ne lasciano inalterato il valore;

- tutte le proprietà essenziali dell'equazione $f(x) = 0$ sono esprimibili nei termini del gruppo G.

Queste poche osservazioni non sono certo sufficienti per valutare l'importanza della teoria di Galois. Un punto tuttavia può essere notato.

All'equazione $f(x) = 0$ viene associata una struttura,– un gruppo finito di permutazioni,– la cui indagine impone un apparato metodologico assai diverso da quello tradizionalmente impiegato nell'analisi delle equazioni prima di Galois.[4]

A partire da Galois, inizia uno studio sistematico dei gruppi di permutazioni, sia in collegamento con le equazioni, sia come oggetti intrinsecamente interessanti.

Ma la centralità del concetto di gruppo, e non solo dei gruppi di permutazioni, emerge anche in molte altre situazioni che tuttavia non possiamo soffermarci a descrivere.[5] Basti dire che a fine Ottocento, come esito naturale di questi risultati matematici, si sviluppa un'assiomatica dapprima per i gruppi finiti poi per i gruppi tout court.

8.3 Il ‘piccolo’ Teorema di Fermat

Il concetto di gruppo (finito) emerge anche in molti altri contesti. Vediamo come la dimostrazione del cosiddetto piccolo teorema di Fermat riesca particolarmente chiara se scopriamo la sua ‘natura gruppale’. Ecco l'enunciato del teorema

Teorema 8. – Sia n un intero arbitrario e sia p un numero primo e primo con n. Allora

$$n^{p-1} \equiv 1 \mod p$$

Oppure: se p primo ed è n qualsiasi si ha

$$n^p - n \equiv 0 \mod p.$$

[4] Con la cospicua eccezione di Lagrange, naturalmente.

[5] Un primo riferimento importante è (Wussing 1984).

Questa prima dimostrazione (di Eulero) è molto semplice, e non richiede alcuna strutturazione algebrica.

Procediamo per induzione: sia $a = 0$. Allora $p\,|0$. Supponiamo il teorema vero per $a = k$. Ossia $p\,|k^p - k$.

$$(k+1)^p = k^p + mp + 1$$

Allora, osservando che ogni coefficiente $\binom{p}{k}$ è multiplo di p se $k \neq 0, 1$,

$$(k+1)^p - (k+1) = (k^p - k) + mp.$$

Per l'ipotesi induttiva $p|k^p - k$ e quindi

$$p|(k+1)^p - (k+1). \quad \Box$$

8.3.1 Un'applicazione dovuta a Fermat

Sia p primo e sia $a^r \equiv 1 \mod p$. Allora se $d = \text{MCD}(r, p-1)$ si ha $a^d \equiv 1 \mod p$. Infatti, possiamo scrivere

$$d = rx + (p-1)y.$$

Quindi

$$a^d \equiv a^{rx+(p-1)y} \equiv (a^r)^x \left(a^{p-1}\right)^y \equiv 1.$$

Siano ora p, q primi e $q\,|2^p - 1$. Allora

$$2^p - 1 \equiv 0 \mod q,\ 2^{q-1} \equiv 1 \mod q$$

Sia $d = MCD(p, q-1)$. Non può essere $d = 1$, ne segue $d = p$ ossia $p|q-1$. Dunque $q \equiv 1 \mod p$. Ma p e q sono dispari. Quindi

$$q \equiv 1 \mod 2p.$$

Consideriamo ora il numero $2^{37} - 1$. Se esso non è primo, dobbiamo cercare i suoi fattori primi solo tra i numeri primi della forma $74k + 1$. Si ha allora

$$2^{37} - 1 = 223 \cdot 616318177.$$

8.3.2 Altre dimostrazioni

Vediamo un'altra dimostrazione del teorema di Fermat (Ivory, 1806).[6]

Se m è primo con n, si ha

$$jn \equiv kn \mod m \Leftrightarrow j \equiv k \mod m$$

Di conseguenza, se p è primo e p è primo con n, i numeri

$$n \mod p, 2n \mod p, \dots (p-1)n \mod p$$

sono $p-1$ numeri diversi, minori di p (non nulli) e quindi sono i numeri $1, 2, \dots p-1$ in un certo ordine. Allora

$$n(2n)\cdots((p-1)n) \equiv$$

$$\equiv (n \mod p)(2n \mod p)((p-1)n \mod p) \equiv$$
$$\equiv (p-1)! \mod p$$

Di conseguenza:

$$(p-1)!\, n^{p-1} \equiv (p-1)! \mod p$$

Siccome $(p-1)!$ non è divisibile per p si può cancellare. $\square$

Ecco ora la dimostrazione che, a giudizio di Eulero era la migliore. Se si considera

$$1, a, a^2, a^3, \dots$$

ove a è primo con p, i resti debbono ripetersi.

$$a^{n+r} \equiv a^r \mod p.$$

Ossia

$$a^r(a^n - 1) \equiv 0 \mod p \Rightarrow a^n \equiv 1 \mod p.$$

Sia n è il minimo intero che verifica questa relazione: gli insiemi

$$\{b, ba, ba^2, \dots, ba^n\}$$

o coincidono o sono disgiunti. Quindi

$$n|p-1.$$

[6]Cfr. (LeVeque 1996, p. 55).

Ossia $p-1=kn$, il che implica

$$a^{p-1} \equiv 1 \mod p.$$

In termini di gruppi: l'ordine di ogni elemento di un gruppo finito G divide l'ordine del gruppo.

Sia p primo: $\mathbb{Z}_p \setminus \{0\}$ è un gruppo moltiplicativo di ordine $p-1$.

La dimostrazione del Teorema dipende da una proprietà molto generale. La natura del numero primo p interviene in modo diverso rispetto alle dimostrazioni precedenti: qui invece occorre osservare che non può essere

$$mn \equiv 0 \mod p$$

se non si ha

$$m \equiv 0 \mod p \quad \vee \quad m \equiv 0 \mod p.$$

Capitolo 9

Sul concetto di funzione

9.1 Il concetto moderno

Il concetto di funzione è fondamentale nella matematica moderna. Una funzione è spesso definita come una 'legge' (prescrizione, procedura, ...) che ad ogni elemento $x \in X$ associa un elemento $y = f(x) \in Y$. Si usano anche spesso i simboli:

$$f : X \longrightarrow Y, \quad x \mapsto f(x).$$

Si può anche eliminare il ricorso 'intuitivo' all'idea di legge e formulare il concetto nei termini (assunti come primitivi) di insiemi e sottoinsiemi: si definisce allora una funzione come il suo grafo, un sottoinsieme del prodotto cartesiano.

$$\begin{aligned}
&f \subset X \times Y \text{ tale che} \\
&\forall x\, \exists y : (x, y) \in f, \\
&(x, y_1) \in f \wedge (x, y_2) \in f \Longrightarrow y_1 = y_2.
\end{aligned}$$

Posta questa definizione, si passa a descrivere le principali proprietà delle funzioni 'astratte'. Si descrivono cioè le funzioni iniettive, suriettive, biunivoche. e si formulano i primi teoremi. Ad esempio: $g \circ f$ iniettiva implica f iniettiva, ecc.

Quando abbiamo X, Y dotati di struttura,– ad esempio se è data in X ed Y una collezione di insiemi da giudicarsi aperti,– possiamo introdurre il concetto di funzione continua, ecc. ...

Questa organizzazione della matematica come insieme di strutture variamente articolate e connesse è concettualmente assai profonda. In quest'ordine

di idee, per esempio, La continuità appare il frutto di una scelta operata sulla struttura dei sottoinsiemi di X e Y. Se tutti i sottoinsiemi di X sono aperti, ogni funzione da X ad Y risulta continua. Diminuendo il numero degli aperti di X certe funzioni non saranno più continue...

Un concetto di funzione è dunque dotato di estrema semplicità ed ha grande potere unificante. Ma *semplice* non vuol dire *facile*. Si giunge alla centralità di questo concetto con Eulero (1749), e il 'motore dello sviluppo' è il calcolo differenziale. Per cogliere dunque l'importanza di questo concetto occorre avere acquisita una certa quantità di esperienza matematica.

Negli *Elementi* di Euclide non è naturale descrivere i risultati in termini funzionali. Si tratta di *costruire* figure con certe caratteristiche; valutare l'*uguaglianza* o l'*equivalenza* di figure; valutare la possibilità di *eseguire certe costruzioni*...

9.2 Nel Seicento

Nella matematica del Seicento, dopo l'introduzione dell'algebra, si ha a che fare con equazioni e manipolazioni di equazioni (cambiamenti di coordinate, intersezione di curve, ecc.). I due problemi principali che danno origine al calcolo, aree e tangenti, sono visti in una prima fase in termini geometrici, dove l'algebra ha un ruolo fondamentale, ma come *strumento*.

Ad un settore parabolico si assegna una *figura equivalente*; non un numero. Data una curva, si individuano delle grandezze geometriche che permettano di *tracciare* la tangente: non si valuta numericamente un'inclinazione.

Nei termini della matematica leibniziana, data una relazione del tipo

$$f(x, y, z, \dots)$$

possiamo ottenere un'altra relazione del tipo

$$\varphi(x, y, z, \dots, dx, dy, dz, \dots)$$

e questa abilità manipolativa corrisponde alla capacità di risolvere un gran numero di problemi: in primis tracciare la tangente ad una curva algebrica. Abbiamo in questo caso una connessione di questo tipo.[1]

$$f(x, y) = 0 \Longrightarrow \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy = 0.$$

[1] Per approfondire la conoscenza della matematica di Leibniz e della sua scuola è tutt'ora fondamentale (Bos 1974).

Newton con i concetti di fluente e flussione è più vicino ad un'idea di funzione; ma nei *Principia* si esprime in termini di quantità geometriche che si danno realmente in natura[2] e tende a relegare la mediazione analitica in un ruolo strumentale (assai diversamente dal precedente *De analysi* degli anni giovanili).

Il concetto di funzione diviene centrale quando ci si interroga su cos'è il substrato del calcolo differenziale. Emergono con chiarezza progressiva questi aspetti:

- È fondamentale l'algoritmo $x^n \mapsto nx^{n-1} = Dx^n$ [3];
- D è lineare;
- ogni quantità 'ragionevole' $f(x)$ può rappresentarsi nella forma

$$f(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Si deriva e si integra liberamente 'termine a termine'.

Nel Settecento non si dà una differenza essenziale tra

$$\sum_{n=0}^{\infty} a_n x^n$$

ed un'espressione costruita con le funzioni elementari come

$$\frac{P(x)}{Q(x)}, \sin x, \cos x, \log x, \exp x, \dots$$

Tra la fine del Settecento e l'inizio dell'Ottocento si pone una nuova esigenza di *rigore*, ed anche questa esigenza pone la necessità di un'analisi profonda del concetto di funzione. L'esigenza di rigore non si dà però astrattamente come una scelta ideologica (o non solo in questo modo).

In una memoria fondamentale,[4] Lagrange ottiene questo risultato: sia $\phi(y)$ un *polinomio*. Allora dall'equazione che definisce (in generale) y come funzione implicita di x

$$y = a + x \cdot \phi(y)$$

[2]Si veda la Praefatio ad lectorem di (Newton 1687).

[3]Ove uso il simbolo D per comodità: in realtà esso è stato introdotto assai più tardi (1800) da Arbogast. Cfr. (Cajori 1993, vol. 2, p. 209)

[4]Cfr. (Lagrange 1770)

possiamo 'invertire' ed ottenere:

$$y = a + \sum_{n=1}^{\infty} \frac{x^n}{n!} \frac{d^{n-1}}{da^{n-1}} [\phi(a)^n]$$

Ad esempio, da

$$y = 1 + xy^2, \tag{9.1}$$

si ottiene

$$y = 1 + x + 2x^2 + 5x^3 + 14x^4 + \dots \tag{9.2}$$

Ma per quali valori di x la (9.2) è convergente? In questo caso è facile rispondere: si osserva che la serie corrisponde ad una delle due radici dell'equazione (9.1(e dunque si ha convergenza per $|x| < \frac{1}{4}$. Tuttavia in casi appena più complessi decidere in merito alla regione di convergenza non è affatto facile.

Poco tempo dopo,[5] Lagrange applica il suo risultato a $\phi(y) = \sin y$, comportandosi come se $\sin y$ fosse un polinomio! Qui il problema della regione di convergenza è ancor più delicato e sarà risolto molto abilmente da Laplace, nella sua *Meccanica Celeste*.

Nelle molteplici occasioni nelle quali Cauchy pone le esigenze di rigore della sua nuova analisi, appare quasi sempre il riferimento alla serie di Lagrange.[6]

Cauchy pone una distinzione radicale tra funzione ed espressione analitica. Non è più possibile di conseguenza definire la derivazione come estensione per linearità. Occorre una definizione indipendente:

$$\lim_{h \to 0} \frac{f(x+h) - f(x)}{h}.$$

9.3 Ancora: storia e insegnamento

In che misura l'insegnamento deve ricapitolare l'esperienza storica? Ecco due casi (a mio giudizio) molto differenti:

- i numeri arabi;
- il concetto di funzione.

[5] In (Lagrange 1769).
[6] Cfr. (Galuzzi 2000).

Operare con i numeri trova un immediato riscontro nella pratica di ogni giorno. L'importanza dell'operare con i numeri arabi si coglie immediatamente. Sarebbe veramente assurdo insegnare ai bambini ad utilizzare i numeri romani per poi giungere, seguendo alla lettera il percorso storico ai numeri attuali. Ma l'operare con i numeri trova, appunto, un immediato riscontro nella pratica quotidiana ed è per questo che appare naturale che le esigenze della vita attuale facciano aggio sulla storia.

Accade lo stesso con il concetto di funzione? Certamente dopo avere detto cos'è una funzione si possono fornire innumerevoli esempi: l'allungamento di una molla, la lunghezza d'un'ombra, l'affrancatura di una busta,... Tutti questi esempi, però, a mio giudizio, hanno carattere retorico. Dopo che un bambino ha imparato che la quantità di denaro che occorre per comprare n oggetti è (prescindendo dai possibili sconti) n-upla di quella che occorre per comprare un singolo oggetto, e che è dunque in presenza della funzione

$$\text{numero degli oggetti} \mapsto \text{numero degli oggetti} \cdot \text{prezzo unitario},$$

non si dà alcun cambiamento rilevante nella sua visione del mondo. L'utilità del concetto di funzione si coglie *solo* nel contesto della pratica matematica avanzata.

9.4 Il contributo della Teoria delle categorie

Tuttavia la pratica quotidiana può essere modificata. A giudizio di F.W. Lawvere, si può fondare la matematica subordinando i concetto elementari ed usuali di insieme e di appartenenza a quello di funzione.[7]

Lawvere ed i suoi allievi sono giunti a queste considerazioni a partire dall'esperienza della Teoria delle Categorie attraverso una riflessione profonda sulla Teoria degli insiemi.[8] Non è possibile dare qui un'idea molto articolata del complesso di ricerche che fanno capo a questa posizione. Ecco però un breve cenno. Possiamo considerare un elemento di un insieme come una funzione particolare

$$x : \{*\} \longrightarrow X,$$

[7]Si veda (Lawvere and Schanuel 1997). Si può anche vedere la precedente edizione italiana (Lawvere and Schanuel 1994) meno soddisfacente, tuttavia, dal punto di vista tipografico.

[8]Cfr. (Lawvere 1999) e (Betti and Lastaria 1997).

ove con $\{*\}$ si intende l'insieme formato da un solo elemento. Non vi sarebbe un gran guadagno se ci si fermasse a questa osservazione banale. Ma anche $\{*\}$ può essere identificato in termini 'funzionali'. Infatti tra un insieme arbitrario Y e $\{*\}$ vi è una sola funzione. La 'Categoria degli Insiemi' ha dunque la particolarità d'avere un oggetto (l'oggetto terminale), che possiamo denotare con $\mathbf{1}$ tale che:

- per ogni insieme X vi è un solo morfismo $X \longrightarrow \mathbf{1}$;
- gli elementi di un insieme X sono i morfismi $\mathbf{1} \longrightarrow X$.

Proseguendo con l'analisi in quest'ordine di idee, si viene a costruire una situazione ove tutte le principali proprietà degli insiemi (Lawvere direbbe 'insiemi astratti') sono riformulate in termini funzionali.

Con quale vantaggio? Il fatto rilevante (e sorprendente)[9] è che da questa analisi si ricavano *proprietà universali* che mostrano aspetti unitari di vari contesti matematici apparentemente assai discosti (ad esempio tra il teorema di Cayley relativo ai gruppi e le sezioni di Dedekind, attraverso il Lemma di Yoneda).

9.4.1 Due piccole osservazioni

L'importanza del concetto di funzione nella matematica moderna implica, talvolta, una certo irrigidirsi su modi 'standard' di risolvere i problemi. Si supponga di voler determinare la tangente all'ellisse di equazione

$$x^2 + 2y^2 = 3$$

nel suo punto $(1, 1)$. Possiamo naturalmente esprimere y come funzione di x, scegliendo opportunamente il segno:

$$y = \frac{1}{2}\sqrt{6 - 2x^2}.$$

Quindi, applicando meccanicamente le regole

$$y' = -\frac{x}{\sqrt{6 - 2x^2}}$$

[9]Un aspetto che amava sottolineare Hardy. Si veda (Hardy 1989, pp. 83–4).

e dunque $y'(1) = -\frac{1}{2}$. Ma possiamo anche scrivere direttamente:

$$2xdx + 4ydy = 0,$$

quindi

$$y' = -\frac{1}{2}\frac{x}{y}.$$

Non vi è alcun vantaggio nell'avere espressa y' nei termini della sola x. Assai più significativo è avere y' nei termini delle due variabili x, y legate dall'equazione dell'ellisse.

Ancora, in non pochi libri, la regola di derivazione di $f(x)^{g(x)}$ è data trasformando opportunamente l'espressione in un'altra (che raramente gli studenti memorizzano). Possiamo scrivere

$$\log y = g(x) \log f(x)$$

Allora

$$\frac{dy}{y} = g'(x) \log f(x)dx + g(x)\frac{f'(x)}{f(x)}dx,$$

e quindi

$$y' = \frac{dy}{dx} = y\left\{g'(x) \log f(x) + g(x)\frac{f'(x)}{f(x)}\right\} = f(x)^{g(x)}\left\{g'(x) \log f(x) + g(x)\frac{f'(x)}{f(x)}\right\}.$$

La modesta conclusione che voglio trarre da questi esempi è che, l'assegnare un legame tra quantità variabili non implica necessariamente che per ogni tipo di problema sia necessario esprimere una di esse in funzione dell'altra. In molti casi è conveniente procedere utilizzando semplicemente il loro legame e rimandando l'eventuale esplicitazione alla fine.

Capitolo 10

Coordinate e geometria

Descartes nel dare inizio alla geometria algebrica, dopo aver introdotto il *segmento unitario*, utilizza liberamente i risultati del Sesto Libro degli *Elementi*[1] per introdurre un calcolo di segmenti le cui operazioni egli pone in corrispondenza con le operazioni algebriche.

Questi segmenti, attraverso un'idea intuitiva e non ancora analizzata di numero reale sono in effetti pensati equivalenti al nostro campo reale.

Nel Settecento la matematica si sviluppa prevalentemente in termini analitici, con una progressiva de-geometrizzazione degli enti matematici. Il rapporto tra geometria e coordinate è privo di problematicità perché le coordinate hanno un ruolo assolutamente prevalente.

Con gli sviluppi dell matematica ottocentesca, l'introduzione sistematica della variabile complessa, le geometrie non euclidee ed il risorgere della geometria proiettiva diviene oggetto d'attenzione critica la ragione per la quale, a partire da un contesto *geometrico* possiamo agire in termini *algebrici*: in altre parole che cosa rende possibile un calcolo di segmenti.

Abbiamo già visto nel Capitolo 6 la sottigliezza dispiegata da Hilbert per analizzare il fondamento di questo calcolo sul quale poggia la geometria analitica attuale.

Ora vogliamo vedere brevemente (e schematicamente) il contributo di Emil Artin.

L'analisi di Artin è molto sottile: invece di istituire un apparato assiomatico che dia ai segmenti, in modo naturale, una struttura algebrica, egli dà un apparato minimale per gli assiomi relativi agli enti geometrici e utilizza

[1] In particolare le proposizioni 10–13.

poi le trasformazioni del piano, le dilatazioni e le traslazioni, per ricostruire il campo attraverso di esso.

Nel seguito riformulo quanto esposto in (Artin 1968, cap. 4).[2]

Sia K un campo.[3] I *punti*, indicati con $A, B, \ldots, P, Q, \ldots$ saranno le coppie ordinate (ξ, η) di elementi di K. Un punto $P = (\xi, \eta)$ sarà anche pensato come un *vettore*. Una *retta* l sarà definita, come insieme di punti, da

$$l = \{X | X = P + tA\}$$

ove P è un punto, A un vettore e $t \in K$. Le frasi "P è un punto di l", "l è parallela ad r", ecc. si interpretano in modo ovvio.

Diremo *dilatazione* una rappresentazione della forma

$$\sigma(X) = \alpha X + C,$$

ove C è un vettore fisso e $\alpha \in K$. Se $\alpha = 0$ si dirà che la dilatazione è *degenere*.

La composizione di dilatazioni è una dilatazione. Sia $\tau(x) = \beta X + D$. Allora

$$\sigma\tau(X) = \sigma(\beta X + D) = \alpha\beta X + \alpha D + C. \tag{10.1}$$

È evidente che l'insieme delle dilatazioni non degeneri forma un gruppo rispetto al prodotto dato dalla composizione. L'unità è data dalla trasformazione identica, che si ottiene per $\alpha = 1$ e $C = \underline{0} = (0, 0)$. L'inversa di σ si calcola immediatamente dalla (10.1).

Tra le dilatazioni non degeneri abbiamo le *traslazioni*, che sono le dilatazioni *prive di punti fissi*. Da

$$X = \sigma(X) = \alpha X + C,$$

posto $C = (a, b), X = (x, y)$ si deducono le condizioni

$$\begin{cases} (1 - \alpha)x = a \\ (1 - \alpha)y = b. \end{cases}$$

[2] Ma inverto l'ordine espositivo. Inoltre per maggiore semplicità considero direttamente un campo invece che un corpo, anche se, come è facile verificare, la commutatività del prodotto non è necessaria.

[3] Si può pensare ad $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ o anche ad un campo di caratteristica finita; o un campo finito o, addirittura $\mathbb{Z}_p$.

Dunque le traslazioni sono individuate da $\alpha = 1$. Indicheremo l'insieme delle traslazioni con $\mathcal{T}$

Se ora scegliamo l'origine $O = (0, 0)$ come punto fisso, tutte le dilatazioni che hanno questo punto come fisso hanno evidentemente la forma

$$\sigma(X) = \alpha X. \tag{10.2}$$

Sia ora $\tau_C(X) = X + C$ una traslazione e si osservi che, se σ è data dalla (10.2) abbiamo

$$\sigma\tau_C\sigma^{-1}(X) = \sigma\tau_C(\alpha^{-1}X) = \sigma(\alpha^{-1}X + C) = X + \alpha C = \tau_{\alpha C}(X). \tag{10.3}$$

Da una traslazione abbiamo ottenuto un'altra traslazione, la quale ha la proprietà importante di avere la stessa direzione della traslazione originaria.[4]

Si noti ora che un elemento $\alpha \in K$ individua esattamente sia una dilatazione della forma (10.2) sia una applicazione

$$\tau_C \mapsto \tau_{\alpha C}$$

dell'insieme $\mathcal{T}$ delle traslazioni in se stesso. Indichiamo l'applicazione individuata da α di $\mathcal{T}$ in $\mathcal{T}$ con τ^α. Si vede allora facilmente che

$$(\tau_1\tau_2)^\alpha = \tau_1^\alpha\tau_2^\alpha$$

e che l'applicazione

$$(\quad)^\alpha : \mathcal{T} \to \mathcal{T}, \qquad \text{data da } \tau \mapsto \tau^\alpha$$

è un omomorfismo.

Indichiamo ora con $(\quad)^0$ l'omomorfismo di $\mathcal{T}$ che ad ogni traslazione associa la traslazione identica e con $(\;)^1$ l'omomorfismo che associa ad ogni traslazione la traslazione stessa.

Sia ora k l'insieme di questi omomorfismi. Possiamo definire la *somma* in k, attraverso la composizione. Se $(\quad)^\alpha, (\quad)^\beta$ sono due elementi di k, dobbiamo vedere come questa somma opera su una traslazione arbitraria τ_C per produrre una nuova traslazione e dunque, ancora, come questa traslazione opera su un punto arbitrario X. Abbiamo allora:

$$\left((\;)^\alpha + (\;)^\beta\right)(\tau_C)(X) = \tau_C^\alpha\left(\tau_C^\beta(X)\right) = \tau_C^\alpha(X + \beta C) = X + \beta C + \alpha C.$$

[4]In termini più 'algebrici': le traslazioni sono un sottogruppo normale del gruppo delle dilatazioni non degeneri.

Dalla definizione posta risulta evidente che

$$(\ )^{\alpha} + (\ )^{\beta} = (\ )^{\alpha+\beta}$$

Analogamente possiamo definire il prodotto: questa volta componendo i morfismi in k con

$$((\ )^{\alpha})^{\beta}.$$

In questo modo k risulta essere organizzato con una struttura di campo. Il campo K risulta posto in corrispondenza di isomorfismo con l'insieme degli omomorfismi k di $\mathcal{T}$ in $\mathcal{T}$ della forma $(\ )^{\alpha}$, attraverso l'applicazione $\alpha \mapsto (\ )^{\alpha}$.

È ora facile vedere che possiamo identificare $k \times k$ con $K \times K$.

L'idea di Emil Artin è ora quella di creare un contesto geometrico sufficientemente ricco per ottenere un insieme di dilatazioni e traslazioni con le proprietà viste. A partire dagli omomorfismi sulle traslazioni si costruirà un *corpo* K, il quale risulterà un campo se, come ha mostrato l'analisi di Hilbert, operiamo una richiesta aggiuntiva su una configurazione geometrica corrispondente ad un caso particolare del teorema di Pascal.[5]

Come Hilbert, Artin parte da due insiemi $\mathcal{P}, \mathcal{R}$ di 'punti' e 'rette' e suppone data una relazione di appartenenza che dia senso a "P giace sul l". Due rette l, m sono dette *parallele* se $l = m$ o se sono prive di punti comuni. Assume poi che per due punti distinti vi sia una sola retta che li contiene e l'assioma di Playfair. Se la retta l contiene $P\ eQ$, Artin scrive

$$l = P + Q.$$

Dopo aver dimostrato che il parallelismo è una *relazione di equivalenza*, chiama *fascio* una classe di equivalenza di rette parallele. Dimostra poi che se esistono tre fasci distinti di rette parallele (almeno tre direzioni) ogni fascio contiene lo steso numero di rette e questo numero è uguale al numero di punti giacenti su una retta qualsiasi.[6] Dopo aver posto l'ulteriore assioma sull'esistenza di almeno tre punti non allineati, si ha la definizione di dilatazione.

[5] Cfr. (Hilbert 1970, cap. 3) o, (Hilbert 1997, cap. 3).
[6] Cfr. (Artin 1968, p. 59).

Definizione 10. – Una rappresentazione

$$\sigma : \mathcal{P} \to \mathcal{P}$$

si chiama dilatazione quando vale la proprietà seguente. Siano P, Q sono punti distinti e sia

$$P' = \sigma(P),\ Q' = \sigma(Q).$$

Sia l' la retta parallela a $P + Q$ passante per P'. Allora Q' giace su l'.

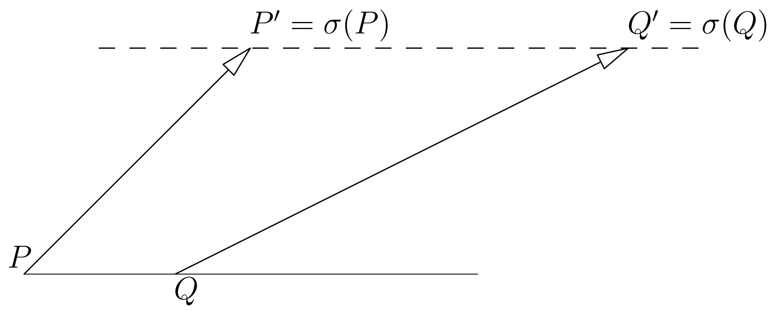


Figura 10.1: Dilatazione

Si dimostra poi facilmente (ma attenzione ad esaminare tutti i casi possibili!) il teorema seguente:

Teorema 9. – Una dilatazione σ è individuata dalle immagini P', Q' di due punti distinti P, Q. Se $P' = Q'$ allora σ manda ogni altro punto in P' (è *degenere*). In caso contrario è una corrispondenza biunivoca.

Corollario 3. – Se una dilatazione ha due punti fissi allora essa è l'identità.

Per individuare le traslazioni, basta ora la definizione seguente (si veda la figura):

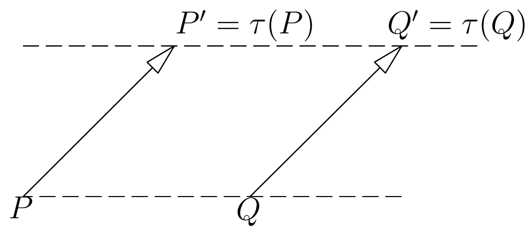


Figura 10.2: Traslazione

Definizione 11. – Una dilatazione non singolare τ si chiamerà *traslazione* se $\tau = 1$ oppure se τ non ha punti fissi.

Sia $\mathcal{T}$ l'insieme delle traslazioni. Procedendo ora 'a ritroso' si tratta di individuare quegli omomorfismi di $\mathcal{T}$ in $\mathcal{T}$ corrispondenti alla (10.3). Ecco una prima definizione:

Definizione 12. – Sia σ una dilatazione non degenere e sia P un punto. Ogni retta contente P e $\sigma(P)$ si dirà una *traccia* di P. Se $P \neq \sigma(P)$ allora la traccia è unica ed è $P + \sigma(P)$.

Figura 10.3: Tracce nei due casi

Per giungere a costruire un corpo K, occorre aggiungere un assioma ulteriore (di evidente significato):

Assioma 1. – Dati due punti P, Q esiste una traslazione τ_{PQ} che porta P in Q.

Ecco ora la definizione fondamentale:

Definizione 13. – Una rappresentazione

$$\alpha : \mathcal{T} \to \mathcal{T}$$

è detta un *omomorfismo che conserva le tracce* se.

(1) è un omomorfismo di $\mathcal{T}$;

(2) conserva le tracce. Più esattamente: $\tau^\alpha = 1$ o τ e τ^α hanno la stessa direzione.

Ora, considerando gli omomorfismi di questo tipo, possiamo costruire un corpo K, definendo la somma ed il prodotto nel modo visto.

Tuttavia per introdurre le coordinate occorre una richiesta ulteriore:[7]

Assioma 2. – Se τ_1, τ_2 sono traslazioni con le stesse tracce e se

$$\tau_1 \neq 1, \tau_2 \neq 1, \tau_1 \neq \tau_2$$

allora esiste un $\alpha \in K$ tale che

$$\tau_2 = \tau_1^\alpha.$$

È ora possibile dimostrare il seguente teorema:

Teorema 10. – Siano τ_1, τ_2 diverse entrambe dall'unità traslazioni con direzioni diverse. Per ogni $\tau \in \mathcal{T}$ esistono e sono univocamente determinati due elementi α, β tali che

$$\tau = \tau_1^\alpha \tau_2^\beta = \tau_2^\beta \tau_1^\alpha.$$

A questo punto, fissata un'origine O e due traslazioni τ_1, τ_2 diverse e diverse dall'unità, dato un punto arbitrario $P = (\alpha, \beta)$ si ha

$$\tau_{OP} = \tau_1^\alpha \tau_2^\beta.$$

Abbiamo un modo per assegnare le coordinate ad ogni punto.

Ancora una volta, la commutatività, come abbiamo osservato, si può far dipendere dal Teorema di Pascal.[8]

[7] Si tratta dell'assioma 4b, cfr (Artin 1968, p.71).

[8] Cfr. (Artin 1968, p. 82).

Bibliografia

Alesina, A., and M. Galuzzi. 1998. "A new proof of Vincent's theorem." *L'Enseignement mathématique* 44:219–256.

Archimede. 1974. *Opere*. Torino: Utet. A cura di A. Frajese.

Artin, E. 1944. *Galois theory*. Notre Dame Lectures, University of Notre Dame Press. Second revised edition.

———. 1968. *Algebra geometrica*. Milano: Feltrinelli. Traduzione italiana di L. Lombardo–Radice e G. Panella.

———. 1988. *Galoissche Theorie*. Thun: Verlag Harri Deutsch. German translation by V. Ziegler.

Artin, M. 1997. *Algebra*. Torino: Boringhieri. Traduzione italiana.

Assayag, G., H.G. Feichtinger, and J.F. Rodrigues, eds. 2002. *Mathematics and music*. Berlin, etc.: Springer.

Ballieu, M. 1942. "Sur le développement des irrationnelles quadratiques en fractions continues régulières." *Mathesis* 54:304–314. Reviewed by I. Niven, MR 7,274c.

Beaulieu, L. 1994. "Dispelling a myth: questions and answers about Bourbaki's early work, 1934-1944." *(?)*. 241–252.

Beltrami, E. 1889. "Un precursore italiano di Legendre e di Lobatschevsky." *Rendiconti Accademia dei Lincei* 5:441–48.

Betti, R., and F. Lastaria. 1997. "Per una concezione dialettica della matematica." *Lettera Matematica* 25:12–14.

Bombelli, R. 1966. *Algebra*. Milano: Feltrinelli. Prima edizione integrale a cura di E. Bortolotti.

Bombieri, E., and A. J. van der Poorten. 1995. "Continued Fractions of Algebraic Numbers." *Computational Algebra and Number Theory.*

Sydney, 1992, Math. Appl. 325. Dordrecht: Kluwer Acad. Publ., 137–152.

Bonola, R. 1975. *La geometria non-euclidea.* Bologna: Zanichelli. Riproduzione anastatica dell'edizione del 1906.

Borges, J.L. 1978. *Finzioni.* Torino: Einaudi. Traduzione italiana di F. Lucentini.

Bos, H.J.M. 1974. "Differentials, higher-order differentials and the derivative in the Leibnizian calculus." *Archive for history of exact sciences* 14:1–90.

Cajori, F. 1993. *A History of mathematical notations.* New York: Dover. Republication in one volume of the work first published in two volumes by The Open Court Publishing Company, La Salle Illinois, 1928 and 1929.

Camilleri, A. 2000. *Un filo di fumo.* Palermo: Sellerio. Tredicesima edizione.

Cassirer, E. 1968. *Storia della filosofia moderna.* Volume 4. Milano: Il Saggiatore di Alberto Mondadori. Trad. italiana di A. Pasquinelli.

Chikara, S., S. Mitsuo, and J.W. Dauben, eds. 1994. *The intersection of history and mathematics.* Basel, Boston, Berlin: Birkhäuser Verlag.

Conway, J.H., and R. Guy. 1999. *Il libro dei numeri.* Milano: Hoepli. Traduzione italiana di A. Zaccagnini.

Corry, L. 1997. "David Hilbert and the axiomatisation of physics (1894-1905)." *Archive for history of exact sciences* 51:83–198.

Croce, B. 1909. *Logica.* Bari: Laterza. Seconda edizione interamente rifatta.

———. 1976. *Teoria e storia della storiografia.* Bari: Laterza. Undicesima edizione.

De Nuccio, S. 2001. "Le frazioni continue aritmetiche e le radici di un'equazione algebrica di 2^o grado. Una memoria di E. Galois." *Periodico di matematiche* 1 (2): 45–63 (aprile-giugno).

Dehn, M. 1900. "Die Legendre'schen Sätze über die Winkelsumme in Dreieck." *Mathematische Annalen* 53:405–439.

Einstein, A. 1967. *Relatività.* Torino: Boringhieri. A cura di B. Cermignani. Con scritti di Descartes, Newton, Lobačevskij, Riemann, Helmholttttz, Maxwell, Poincaré, Einstein.

Enriques, F., ed. 1924 - 27. *Questioni riguardanti le matematiche elementari.* Bologna: Zanichelli. Riproduzione anastatica, Zanichelli, Bologna, 1983.

Escofier, J.-P. 2001. *Galois theory.* New York, etc.: Springer.

Euclide. 1970. *Elementi.* Torino: Utet. Traduzione italiana a cura di A. Frajese e L. Maccioni.

Euler, L. 1774 (1773). *Elémens d'algèbre.* Lyon: J.-M. Bruset. Traduction française.

———. 1988. *Introduction to the Analysis of the infinite.* New York: Springer-Verlag. English translation by J.D. Blanton.

Ferreira, M. P. 2002. "Proportions in ancient and medieval music." *(?).* 1–25.

Festa, E., and R. Gatto, eds. 2000. *Atomismo e continuo nel XVII secolo.* Napoli: Vivarium.

Fowler, D.H. 1987. *The mathematics of Plato's Academy.* Oxford: ClarendonPress.

Galilei, G. 1970. *Dialogo sopra i due massimi sistemi del mondo.* Torino: Einaudi. A cura di L. Sosio.

Galois, E. 1976. *Écrits et mémoires mathématiques d'Évariste Galois.* Paris: Gauthier-Villars. Par R. Bourgne et J. P. Azra, Préface de J. Dieudonné. Deuxième édition revue et augmenté. Réimpression autorisé, Editions J. Gabay, 1997.

Galuzzi, M. 1995. "Forse basta dirlo." *Lettera Pristem* 18:9–10.

———. 1999a. "Caratteri specifici della tradizione matematica italiana." *Italia: origini aspetti e problemi di una identità nazionale.* Milano: Istituto lombardo di scienze e lettere. Lezioni di varî autori tenute nell'anno 1997/98.

———. 1999b. "Fondamenti, che passione." *Lettera matematica Pristem* 33-34:81–84.

———. 2000. "La continuità: da proprietà ad attributo nella matematica dal Settecento ad oggi." *in (?).* 87–106.

———. 2001. "Diffusione e critica di Bourbaki in Italia nel secondo dopoguerra." Edited by G. Anichini, *Notiziario della Unione Matematica Italiana. XXI Convegno nazionale UMI-CIIM sull'insegnamento della matematica. "Nuclei fondanti del sapere matematico nella scuola del 2000 (in ricordo di Francesco Speranza), Salsomaggiore Terme, 13-14-15 aprile 2000.* Edizioni dell'Unione Matematica Italiana.

———. 2002. "Descartes e la geometria analitica." *Bollettino della Sezione Mathesis di Milano* 9:18–34.

Galuzzi, M., and M. Neubrand. 1998. "Appendix: influences of history and the general social development on teaching of geometry." In *Perspectives on the teaching of geometry for the 21st century. An ICMI study*, edited by C. Mammana and V. Villani, 229–234. Dordrecht: Kluwer Academic Publishers.

Galuzzi, M., M. Neubrand, and C. Laborde. 1998. "The evolution of the curricula as indicated by different kinds of change in geometry textbooks." In *Perspectives on the teaching of geometry for the 21st century. An ICMI study*, edited by C. Mammana and V. Villani, 204–222. Dordrecht: Kluwer Academic Publishers.

Galuzzi, M., and D. Rovelli. 1997. "Storia della geometria e didattica: qualche osservazione." In *Quaderno 19/2 del Ministero della Pubblica Istruzione. L'insegnamento della geometria*, 70–110. Lucca: Liceo scientifico statale *A. Vallisneri.*

Graham, R.L., D.E. Knuth, and O. Patashnik. 1989. *Matematica discreta.* Milano: Hoepli. Traduzione italiana.

Hardy, G.H. 1989. *Apologia di un matematico.* Milano: Garzanti. Traduzione di L. Saraval. Presentazione di E. Vesentini.

Hardy, G.H., and E.M. Wright. 1971. *An Introduction to the Theory of Numbers.* Oxford: Oxford University Press. Fourth edition.

Hilbert, D. 1899. "Grundlagen der Geometrie." *Festschrift zur Feier der Enthüllung des Gauss-Weber-Denkmals in Göttingen.* Leipzig: Teubner.

———. 1970. *Fondamenti della geometria.* Milano: Feltrinelli. Trad. it. a cura di P. Canetta. Con i supplementi di Paul Bernays.

———. 1997, Second English edition. *Foundations of Geometry.* La Salle - Illinois: Open Court.

Kant, I. 1959. *Primi principi metafisici della scienza della natura.* Urbino: Cappelli. Introduzione di L. Geymonat. Nota informativa e traduzione di L. Galvani.

Kline, M. 1991. *Storia del pensiero matematico.* Torino: Edizione italiana a cura di A. Conte, 2 volumi, Einaudi.

Knorr, W.R. 1975. *Evolution of the Euclidean Elements.* Dordrecht: Reidel.

Koyré, A. 1972. *Studi newtoniani.* Torino: Einaudi. Traduzione italiana di P. Galluzzi.

———. 1976. *Studi galileiani.* Torino: Enaudi. Traduzione italiana di M. Torrini.

Křížek, M., F. Luca, and L. Somer. 2001. *17 Lectures on Fermat numbers.* New York: Springer.

Lagrange, J.L. 1769. "Sur le problème de Kepler." *Histoire de l'Académie royale des Sciences et des Belles–Lettres (Berlin)* 25 (1771) (In Œuvres III, pp. 113-138.): 204–233.

———. 1768 (1770). "Nouvelle méthode pour resoudre les équations littérales par le moyen des séries." *Histoire de l'Académie Royale des Sciences et Belles-Lettres (de Berlin)* 24:251–326. *Œuvres* 3: 5-73.

———. 1867–1879. *Œuvres.* Edited by J.-A. Serret. Paris: Gauthier-Villars.

Lawvere, F. W., and S.H. Schanuel. 1997. *Conceptual mathematics. A first introduction to categories.* Cambridge: Cambridge University Press.

Lawvere, F.W. 1999. "Categorie e spazio: un profilo." *Lettera Matematica* 31:35–50.

Lawvere, F.W., and S.H. Schanuel. 1994. *Teoria delle categorie: un'introduzione alla matematica.* Franco Muzzio editore. Edizione italiana a cura di A. Carboni.

LeVeque, J. 1996. *Fundamentals of Number Theory.* New York: Dover. Unabridged, unaltered republication of the work first published by the Addison-Wesley Publishing Company, Reading, Massachusetts, 1977.

Lobačevskij, N. 1974. *Nuovi principi della geometria.* Torino: Boringhieri. A cura di L. Lombardo Radice.

Lorentzen, L., and H. Waadeland. 1992. *Continued fractions with applications.* Amsterdam -London - New York - Tokio: North-Holland.

Loria, G. 1923. "Da Descartes e Fermat a Monge e Lagrange. Contributo alla storia della geometria analitica." *Reale Accademia dei Lincei. Atti. Memorie della classe di scienze matematiche fisiche e naturali (5)* 14:777–485.

Mangione, C., and S. Bozzi. 1993. *Storia della logica.* Milano: Garzanti.

Mugler, C. 1958. *Dictionnaire historique de la terminologie géométrique des grecs.* Paris: Librairie C. Klincksieck.

Newton, I. 1687. *Philosophiae naturalis Principia Mathematica.* Iussu Societatis regiae ac Typis Josephi Streater. Impression anastaltique Culture et Civilisation, Bruxelles, 1965.

Olds, C. D. 1968. *Frazioni continue.* Bologna: Zanichelli. Traduzione italiana a cura di F. Speranza.

Panza, M. 2002. "I metodi matematici nelle scienze umane." *Lettera matematica Pristem*, pp. 31–40.

Petsinis, T. 1997. *The French mathematician.* New York: Walker and Company.

Pirandello, L. 1937–38. *Novelle per un anno.* Milano: Mondadori. In 2 volumi. Comprende tutti i volumi dell'edizione Bemporad-Mondadori.

———. 1993. *La mosca.* Milano: Mondadori. A cura di Simona Costa.

Rockett, A.M., and P. Szüs. 1992. *Continued Fractions.* Singapore, ecc.: World Scientific.

Rothman, T. 1982. "Genius and biographers: the fictionalization of Evariste Galois." *American Mathematical Monthly* 89:84–106.

Rotman, J. 1998. *Galois theory.* New York, ecc.: Springer-Verlag. Second edition.

Saccheri, G. 1986. *Euclides vindicatus.* New York: Chelsea publishing company. Edited and translated by G.B. Halsted.

Scimone, A. 1997. *La sezione aurea.* Palermo: Sigma edizioni.

Stillwell, J. 2002, Second edition. *Mathematics and its history.* New York, etc.: Springer.

Toepell, M. 1986. "On the origins of David Hilbert's *Grundlagen der Geometrie*." *Archive for history of exact sciences* 35:329–344.

Toth, I. 1997. *Aristotele e i fondamenti assiomatici della geometria.* Milano: Vita e pensiero. Prefazione e Introduzione di G. Reale. Trad. di E. Cattanei.

Toti Rigatelli, L. 1996. *Evariste Galois.* Basel: Birkhäuser Verlag. Translated from the Italian by John Denton.

Trudeau, R.J. 1987. *The non-Euclidean revolution.* Boston; Basel; Stuttgart: Birkhäuser.

Vailati, G. 1903. "Di un'opera dimenticata del P. Gerolamo Saccheri ("Logica demonstrativa" 1697)." *(?).* Originariamente apparso nella Rivista Filosofica.

———. 1987. *Scritti, 3 volumi.* Bologna: Arnaldo Forni editore. A cura di M. Quaranta.

Weil, A. 2002. "Storia della matematica: perché e come." *Collana LIDIM del Dipartimento di Matematica dell'Università di Milano* 4:1–30. Traduzione italiana a cura di M. Galuzzi.

Wilf, H.S. 1994, Second edition. *Generatingfunctionology.* Boston, ecc.: Academic Press, Inc.

Wussing, H. 1984. *The genesis of the abstract group concept.* Cambridge, Massachusetts: The MIT Press.